Bayerisches Landesamt für
Datenschutzaufsicht

12. Tätigkeitsbericht

2022

12. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für das Jahr 2022

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: KI generiertes Bild zum Schlagwort „Guardian of a Fundamental Right“

Vorgelegt im Juli 2023 – Michael Will, Präsident

Datenschutzjahr 2022 – wo stehen wir?

„Das Jahr der Zeitenwende" – das ist eines der Prädikate, das in künftigen Geschichtsbüchern untrennbar mit dem Jahr 2022 und all seinen durch den russischen Angriffskrieg auf die Ukraine ausgelösten politischen und wirtschaftlichen Veränderungen verknüpft bleiben wird. Es gilt – maßstäblich verkleinert – auch für das Datenschutzjahr 2022, das dieser 12. Tätigkeitsbericht des Landesamts für Datenschutzaufsicht behandelt.

Auf der Schwelle der neuen Datenökonomie

Anders als für die Weltpolitik mit dem 24. Februar 2022 ist der Wendepunkt des Datenschutzjahrs 2022 kaum taggenau fixierbar. Als einer der symbolträchtigsten Anknüpfungspunkte bietet sich freilich der 30. November 2022 an. An diesem Tag wurde der Chatbot ChatGPT erstmals der Öffentlichkeit zugänglich gemacht. Er dient heute zugleich als Anlass und Musterbeispiel zahlloser Debatten über Künstliche Intelligenz (KI). Die Bereitstellung des Dienstes durch das US-Unternehmen OpenAI kann als Beginn der Massenanwendung auf KI basierender Dienste betrachtet werden. Auch wenn die hierdurch ausgelösten und stetig anschwellenden gesellschafts- und rechtspolitischen Diskussionen rund um die mannigfaltigen Schattierungen des Themas „Künstliche Intelligenz" sowie die alsbald mit diesem Dienst verbundenen datenschutzaufsichtlichen Verfahren erst Gegenstand des nächsten Berichtszeitraums sein werden, so prägt dieses Datum doch bereits das Jahr 2022.

Neben einem weiteren Technologiesprung steht die Bereitstellung von ChatGPT und weiterer KI-assoziierter Anwendungen für ein breites Publikum stellvertretend für den Auftakt zur globalen und europäischen Datenökonomie, also der zielgerichteten Nutzung von Daten als Grundlage für Forschung und Innovation.

Die Förderung und Regulierung dieser Datenökonomie steht im Mittelpunkt einer mittlerweile kaum noch überschaubaren Anzahl von Initiativen und Gesetzesvorhaben auf nationaler wie auch europäischer Ebene – etwa dem Dateninstitut der Bundesregierung oder den europäischen Großprojekten wie dem EU-Datengesetz, dem EU-Gesundheitsdatenraum oder der EU-Verordnung zu Künstlicher Intelligenz. Gleichzeitig erprobt nicht nur die Tech-Industrie sondern immer mehr auch Unter-nehmen klassischer Branchen aller Größen - teils vorsichtig, teils forsch – die Nutzung und den Nutzen von KI zur Unterstützung und Fortentwicklung der eigenen Geschäftsprozesse, Produkte und Dienstleistungen.

Wo steht die Datenschutzaufsicht in der Welt der Datenökonomie?

Artikel 8 der Charta der Grundrechte der Europäischen Union weist den europäischen Datenschutzaufsichtsbehörden eine besondere Rolle zu. Sie sind - so eine häufig zu hörende Metapher - „Guardian of a Fundamental Right", die Hüterinnen des Grundrechts auf Schutz personenbezogener Daten. Da die Datenökonomie ohne die Nutzung personenbezogener Daten weder sinnvoll noch beabsichtigt sein kann, schaffen diese Entwicklungen unvermeidbar zusätzliche Aufgaben und Herausforderungen für die Datenschutzaufsichtsbehörden.

Dies beginnt mit der Beratung des Gesetzgebers, beispielsweise mit der aus heutiger Sicht immer noch zielgenauen Entschließung der Datenschutzkonferenz aus dem Jahr 2019, der sog. Hambacher Erklärung zu Künstlicher Intelligenz, und endet nicht bei den jüngsten EDSA-Stellungnahmen etwa zum EU-Datengesetz oder dem EU-Gesundheitsdatenraum.

Weitere Aufgaben, insbesondere aber Herausforderungen, stellen sich bei der technischen

und (datenschutz-) rechtlichen Analyse der neuen Technologien sowie der Sensibilisierung für den Datenschutz in der alltäglichen Praxis.

Auch wenn die genauen Einzelheiten zur Rolle der Datenschutzaufsichtsbehörden noch nicht abschließend ausbuchstabiert sein mögen, so ist doch angesichts des Kontrollauftrags durch Art. 8 der Grundrechtecharta klar: ohne eine Beteiligung der Datenschutzaufsichten werden auch in der künftigen Datenökonomie datenschutzrechtliche Herausforderungen nicht bewältigt werden können.

Schlussanträge in der Rechtssache C-252/21 vom 20. September 2022 – „Meta – Bundeskartellamt"

„So unterliegt eine Wettbewerbsbehörde, wenn sie die Bestimmungen der DSGVO auslegt, in Ermangelung präziser Regeln über die Mechanismen der Zusammenarbeit, die gegebenenfalls vom Unionsgesetzgeber zu erlassen sind, zumindest Informations-, Auskunfts- und Kooperationspflichten […]

Darüber hinaus obliegt es der Wettbewerbsbehörde in Ermangelung einer Entscheidung der zuständigen Aufsichtsbehörde gleichwohl, diese zu informieren und mit ihr zusammenzuarbeiten, wenn diese Behörde mit der Untersuchung derselben Praxis begonnen oder ihre Absicht, dies zu tun, bekundet hat, sowie gegebenenfalls das Ergebnis der Untersuchung durch diese Behörde abzuwarten, bevor sie ihre eigene Beurteilung vornimmt, soweit dies angemessen ist und insbesondere die Einhaltung einer angemessenen Untersuchungsfrist durch die Wettbewerbsbehörde und die Verteidigungsrechte der betroffenen Personen unberührt lässt.

Klare Fingerzeige hierzu lassen sich der jüngst vom EuGH getroffenen Entscheidung zur datenschutzrechtlichen Bewertungen des Marktverhaltens von Meta (vormals „Facebook") durch das Bundeskartellamt entnehmen. In der vom EuGH bestätigten Analyse des Zusammenspiels zwischen datenschutzaufsichtlicher und wettbewerbsbehördlicher Kontrollzuständigkeit durch den Generalanwalt finden sich Anforderungen an Kooperation, Information und Beteiligung, die bereits als Blaupause für die Zuständigkeitsstruktur einer künftigen Regulierung von Datennutzungsrechtsakten bis hin zur Genehmigung von Hochrisiko-KI durch andere als unabhängige Aufsichtsbehörden gelesen werden dürfen. Für die Datenschutzaufsichts-behörden bedeutet dies: egal ob Genehmigung von Datenflüssen im EU-Gesundheitsdatenraum oder Trainings-daten für KI-Modelle – sie werden sich damit befassen müssen.

Angesichts dieser Zukunftsperspektiven ziert das Titelbild des diesjährigen Berichts erstmals ein KI-Erzeugnis, ein durch einen Prompt im KI-Dienst Midjourney geschaffenes Bildnis einer europäischen Wächterin des Datenschutzgrundrechts.

Datenschutzaufsicht im Jahr 5 der DS-GVO – „bedingt handlungsfähig"?

Auch unabhängig von all diesen zukünftigen Aufgaben und Herausforderungen der darf das Jahr 2022 als ein Wendepunkt der bayerischen Datenschutzaufsicht betrachtet werden: Erstmals seit Geltungsbeginn der DS-GVO weist die Eingangsstatistik des Landesamts bei nahezu sämtlichen wesentlichen Kennzahlen leicht rückläufige Trends auf.

Unbeschadet einer vertieften Analyse (Näheres dazu in Kapitel 2 „Zahlen und Fakten") macht ein Blick in die bereits vorliegenden Tätigkeitsberichte auch anderer deutscher Aufsichtsbehörden deutlich, dass der Rückgang der Eingangszahlen im Jahr 2022 kein bayerischer Sondereffekt ist. Bundesweit können als eine der naheliegenden Ursachen sicherlich die im zurückliegenden Jahr in den Vordergrund getretenen, existentiellen Themen wie Inflation oder Energieversorgung betrachtet werden.

Der moderate, aber gleichmäßige Rückgang bei Beschwerden, Meldungen von Datenschutzverletzungen und Beratungsanfragen steht andererseits auch in Übereinstimmung mit einem, an verschiedenen weiteren Entwicklungen ablesbaren Grundbefund der aufsichtlichen Praxis: Im fünften Jahr ihrer Geltung haben sich die DS-GVO und ihre Anforderungen an die Datenverarbeitungsprozesse in Unternehmen und Vereinen mittlerweile als weitgehend stabiler Standard etabliert. Dies gilt im Übrigen genauso für die erst seit 1. Dezember 2021 mit dem Telekommunikations- und Telemediendatenschutzgesetz (TTDSG) gesetzlich klar geregelten Anforderungen zum Einsatz von Cookies auf Webseiten und anderen Zugriffen auf Endeinrichtungen. Der diesbezügliche Rückgang des Beschwerdeaufkommens zeigt überdeutlich den Erfolg einer in Deutschland viel zu lange verzögerten rechtssicheren Umsetzung europäischer Vorgaben zum Schutz der Privatsphäre in der elektronischen Kommunikation.

Weniger, aber komplexere Vorgänge

Für den aufsichtlichen Alltag bedeutet dies, dass Basisthemen zur grundlegenden Umsetzung der DS-GVO in Unternehmen oder Vereinen mehr und mehr in den Hintergrund treten. An ihre Stelle treten komplexere Fragestellungen, die letztlich nur durch intensive Einzelfallprüfung beantwortet werden können - trotz aller nachvollziehbaren Erwartungen von Unternehmen und Verbänden auf einfache, möglichst generelle und binäre „ja/nein" bzw. „zulässig/unzulässig" – Antworten.

Das Erfordernis einer intensiven, strikt am jeweiligen Einzelfall ausgerichteten Prüfung und Bewertung, etwa bei den vielfältigen Möglichkeiten der Konfiguration von Standard-Tools, bei Drittstaatentransfers, bei Datenpannen-Meldungen oder bei der Bewertung von Pseudonymisierungs- und Anonymisierungsmaßnahmen, hat unmittelbare Rückwirkungen auf den aufsichtlichen Prüfaufwand und auch die Verfahrensdauer - und damit letztlich die Entwicklung der Abschluss- und Erledigungskennzahlen.

Gerade auch deshalb verharren die Zahl der unerledigten Fälle wie bereits schon in den Vorjahren auf einem inakzeptabel hohen Stand von zuletzt mehr als 4.000 (siehe im Einzelnen Kapitel 2 zum „Schuldenberg"). Das von der DS-GVO gesetzte Drei-Monatsziel für Beschwerdeverfahren (vgl. Art. 78 Abs. 2 DS-GVO) wird in statistisch rund einem Drittel aller Verfahren nicht erreicht. Die ausbleibende Verbesserung dieser Leistungskennzahlen, trotz erstmaligen Rückgangs der Eingangszahlen, ist im fünften Jahr der DS-GVO ein deutliches Warnsignal. Sie belegt letztlich ein strukturelles Missverhältnis zwischen Aufgabenbelastung und haushaltsrechtlich zugewiesenen Ressourcen.

Zwanzig Jahre nach seiner Errichtung als zentrale Datenschutzaufsichtsbehörde für Unternehmen und Vereine in Bayern darf das Team des Landesamts mit Dankbarkeit und Stolz auf seine Vergangenheit zurückschauen, wie auch das im Juni des Berichtsjahrs mit hochrangigen Gästen aus Politik und Praxisvertretern aus Aufsicht, Wirtschaft und Wissenschaft in einem Symposium gefeierte Gründungsjubiläum eindrucksvoll vor Augen geführt hat.

Unter Berücksichtigung der im Berichtszeitraum auf den Weg gebrachten, heute bestätigten Haushaltsentscheidungen für das Jahr 2023, besteht für das Landesamt Anlass für eine kritische Prüfung seiner eigenen Zukunftsfähigkeit.

Erwartungen an die Datenschutzaufsicht

Die Bindung aufsichtlicher Ressourcen im Bereich der Beschwerdebearbeitung ist angesichts der Rolle der Aufsichtsbehörden als Unterstützung Betroffener bei der Durchsetzung ihrer grundrechtlichen Schutzansprüche gegen Verantwortliche fraglos gerechtfertigt – mehr noch: sie ist vor dem Hintergrund der zunehmenden Anerkennung eines individuellen Anspruchs auf wirksame aufsichtliche Maßnahmen durch die Rechtsprechung mit allen daraus resultierenden

Konsequenzen bis hin zur Zuerkennung eines Überprüfungsanspruchs hinsichtlich der Angemessenheit einer Bußgeldentscheidung gegen den Verantwortlichen der Disposition der Aufsichtsbehörden zunehmend entzogen.

Schlussanträge in den Rechtssachen C-26/22 und C-64/22 vom 16. März 2023 – „Land Hessen/SCHUFA"

„Auch wenn die Aufsichtsbehörde als Garantin für die Einhaltung der Bestimmungen der DSGVO verpflichtet ist, sich mit den bei ihr eingelegten Beschwerden zu befassen, sprechen mehrere Gesichtspunkte für eine Auslegung, wonach sie bei der Prüfung der Beschwerden über ein Ermessen sowie einen gewissen Handlungsspielraum bei der Wahl der geeigneten Mittel zur Erfüllung ihrer Aufgaben verfügt. […] Die detaillierte Beschreibung der Befugnis der Aufsichtsbehörden, Abhilfemaßnahmen zu erlassen, zeigt, dass der Unionsgesetzgeber nicht das Ziel verfolgt hat, das Beschwerdeverfahren zu einem petitionsähnlichen Verfahren zu machen. Vielmehr scheint es das Ziel des Gesetzgebers gewesen zu sein, einen Mechanismus zu schaffen, der geeignet ist, die Rechte und Interessen der Personen, die Beschwerden einlegen, wirksam zu wahren.

CURIA - Dokumente (europa.eu)

Anders als bei der in der Vergangenheit verbreiteten Einordnung des datenschutzrechtlichen Beschwerdeverfahrens als Petitionsrecht, räumt die DS-GVO nach einem bereits in den Schlussanträgen des EuGH-Generalanwalts ablesbaren unionsrechtlichen Verständnis den Betroffenen einen echten, auch im Verhältnis zu Unternehmen anwendbaren „verwaltungsrechtlichen Rechtsbehelf" ein, der keinen nennenswerten Spielraum für Opportunitätserwägungen oder Gewichtungen für datenschutzrechtliche Risiken belässt.
In der künftigen aufsichtlichen Praxis werden daher die Beschwerdevorgänge zunehmen oder doch zumindest auf heutigem Niveau verharren, schon weil dies den aus Sicht des Betroffenen günstigsten und risikoärmsten Weg für eine Rechtsdurchsetzung verspricht.

Das Leistungsversprechen auf umfassende staatliche Prüfung erhöht im Übrigen mittelbar auch die Anforderungen an die Verfahrensgestaltung (z.B. im Hinblick auf Anhörungs- oder Begründungserfordernisse für ergriffene oder verworfene Abhilfemaßnahmen) und stellt damit derzeitige Verfahrensvereinfachungen wie z.B. den umfassenden Ausschluss des Akteneinsichtsrechts Betroffener durch Art. 20 Abs. 2 BayDSG absehbar auf den Prüfstand.

Für die Erfüllung der anderen Angelegenheiten aus dem insgesamt 21 weitere Positionen umfassenden Katalog aufsichtlicher Aufgaben (Art. 57 Abs. 1 DS-GVO) verbleibt angesichts der gesetzlichen Priorisierung des Beschwerdeverfahrens damit immer weniger Spielraum. Für Verantwortliche bedeutet dies, dass etwa eine Genehmigungsentscheidung im Rahmen der Prüfung unternehmensinternen Datenschutzvorschriften nach Art. 47 DS-GVO schon heute beim Landesamt bis zu 24 Monate beanspruchen kann. Nichts anderes ist bei kleinen oder mittleren Unternehmen zu erwarten, sobald diese beginnen, von dem in der DS-GVO als Beitrag zur Rechtssicherheit verankerten Instrument der Zertifizierungen oder der Möglichkeit von Verhaltensregeln Gebrauch zu machen. Auch insoweit erfordert etwa die Prüfung von Zertifizierungskriterien eine abschließende Genehmigung durch das Landesamt (Art. 43 Abs. 2 DS-GVO), für das mit seiner heutigen Ressourcenausstattung ein solches Verfahren nicht bewältigbar wäre.

Transparenz als Grundbedingung aufgabengerechter Ressourcen

Seit Geltungsbeginn der DS-GVO hat das Landesamt im Rahmen seiner regelmäßigen Beteiligung an der Aufstellung des Staatshaushalts durch die Staatsregierung auf diese Zielkonflikte und Ressourcenengpässe stetig und u.a.

durch die Anmeldung von Personalstellen aufmerksam gemacht. Dennoch verharrt das Landesamt auch heute noch in seiner Ursprungsstruktur - als wäre es weiterhin nur ein aus der Regierung von Mittelfranken herausgelöstes Sachgebiet mittlerer Größe. Anders als sonst beim Aufbau neuer Behörden, hat der konsequente haushaltsrechtliche Aufbau als eigenständig handlungsfähige und aufgabengerecht ausgestatten Organisationseinheit bislang nicht stattgefunden.

Diese, originär schon unabhängig von der DS-GVO bestehenden Entwicklungserfordernisse wurden in den Haushaltsjahren 2017 bis 2021 mit Aufstockungen des Ausgangsbestandes von 16 Planstellen auf zuletzt 33 Planstellen wenigstens noch in kleinen, kontinuierlichen Schritten durchaus umgesetzt. Der Haushaltsplan für das Jahr 2022 sah dann aber weder Stellenzuwächse noch Stellenanhebungen für das LDA vor.

Im selben Zeitraum verzeichnet der Staatshaushalt beispielsweise alleine mit dem Landesamt für Sicherheit und Informationstechnik, dem Landesamt für Asyl und Rückführung oder dem Landesamt für Pflege bedeutende Neugründungen, einhergehend mit beträchtlichen Personalaufwüchsen. Dabei setzte doch gerade die zum Jahresende 2022 im Bayerischen Staatsministerium des Innern und für Sport angekündigte, zusätzliche Abteilung für Digitalisierung und Datenschutz ebenfalls ein Signal – das Signal, dass nicht nur bei der Stärkung der Verwaltungsdigitalisierung, sondern auch der Stärkung des Datenschutzes „neue Schwerpunkte“ gesetzt werden sollen. Dennoch enthielt der zur selben Zeit von der Staatsregierung mit der Ausbringung von mehr als 3.000 zusätzlichen Planstellen ins Haushaltsverfahren eingebrachte und im Frühjahr 2023 vom Landtag verabschiedete Haushaltsplan 2023 nicht eine einzige der für das Landesamt für Datenschutzaufsicht angemeldeten 28 Planstellen.

Vorbild Transparenzgebot in § 29 Abs.3 BHO

Weicht der Entwurf des Haushaltsplans von den Voranschlägen der Bundespräsidentin oder des Bundespräsidenten, des Deutschen Bundestages, des Bundesrates, des Bundesverfassungsgerichts, des Bundesrechnungshofes oder der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit ab und ist der Änderung nicht zugestimmt worden, so sind die Teile, über die kein Einvernehmen erzielt worden ist, unverändert dem Entwurf des Haushaltsplans beizufügen.

Beginnend mit diesem Bericht wird das Landesamt seine Haushaltsanmeldungen künftig im Rahmen des jährlichen Tätigkeitsberichts veröffentlichen. Damit wird ausgeglichen, dass das bayerische Haushaltsrecht anders als das des Bundes keine Transparenz für die Stellenanmeldungen der unabhängigen Datenschutzaufsichtsbehörden vorsieht.

Pressemitteilung des Bayer. Staatsministeriums des Innern vom 23. Juni 2022

"Mit zusätzlichen Stellen und einer verbesserten Ausstattung im nächsten Haushalt stellen wir sicher, dass das Landesamt auch weiterhin die vielfältigen Aufgaben und Befugnisse effektiv wahrnehmen kann und für sämtliche künftige Herausforderungen bestens gerüstet ist.“

Der seit Geltung der Offenlegungsverpflichtungen des § 29 Abs. 3 der Bundeshaushaltsordnung vollzogene Stellenaufwuchs der bzw. des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von 90 Stellen in 2016 bis hin zu derzeit 424 Stellen zeigt, dass Transparenz im Haushaltsverfahren einen wesentlichen Beitrag dazu leisten kann, den Haushaltsgesetzgeber für die Handlungserfordernisse unabhängiger, nicht unmittelbar an den Entscheidungsprozessen der Haushaltseinbringung und -beratung beteiligten Aufsichtsbehörden zu sensibilisieren.

2023 als Jahr der Trendwende?

Fünf Jahre nach Geltungsbeginn der DS-GVO und mehr als zwanzig Jahre nach der Entscheidung für die Einrichtung einer unabhängigen Datenschutzaufsichtsbehörde für Unternehmen und Vereine sind rasche Weichenstellungen für die weitere Fortentwicklung des Landesamts geboten.

Digitalplan Bayern 2030

„Um innovative Datennutzung zu ermöglichen und dadurch neue Geschäftsmodelle zu fördern, bauen wir das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) weiter zu einem Kompetenzzentrum für den Datenschutz aus. Die Beratungsfunktion des BayLDA insbesondere für KMUs, Start-ups, Vereine und ehrenamtlich Tätige wird weiterhin einen wichtigen Stützpfeiler bilden, während das BayLDA gleichzeitig zügig neue Instrumente wie Zertifizierungen, Verhaltensregeln (Codes of Conduct) oder verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) für in Bayern ansässige Unternehmen genehmigen können soll. Zudem soll es mit den nötigen personellen Ressourcen ausgestattet werden, um wichtige Weichenstellungen auf EU-Ebene im Sinne Bayerns mitzugestalten."

Aus Sicht des Landesamts erfordert die wirksame und für Betroffene ebenso wie für Unternehmen und Vereine produktive, konstruktive und zukunftsgewandte Erfüllung seiner Aufgaben, einschließlich der Bereitstellung präventiver Beratung als stabiler, Rechtssicherheit vermittelnder Rahmen der Digitalisierung, beschleunigte Aufbauschritte mit dem klaren Ziel, kurzfristig mindestens eine Verdoppelung der heute zur Verfügung stehenden Ressourcen zu erreichen.

Die Antwort auf die Frage, ob dieses Ziel durch den bayerischen Haushaltsgesetzgeber bestätigt und umgesetzt wurde, bleibt dem Tätigkeitsbericht für das Jahr 2023 vorbehalten. Bisher liegen mit der Ankündigung des für den Haushaltsplan des Landesamts zuständigen Staatministers Herrmann im Rahmen des Gründungsjubiläum des Landesamts und dem durch den Ministerrat gebilligten Digitalplan Bayern 2030 schon Zielvorgaben und Strategien vor., Diese bedürfen nunmehr der Unterstützung des Haushaltsgesetzgebers.

Ansbach, im Juli 2023

Michael Will
Präsident

Inhaltsverzeichnis

1

Datenschutzaufsicht im nicht-öffentlichen Bereich

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Gesetzliche Grundlage für den Tätigkeitsbericht

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

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

1.2 Datenschutz in Bayern

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

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

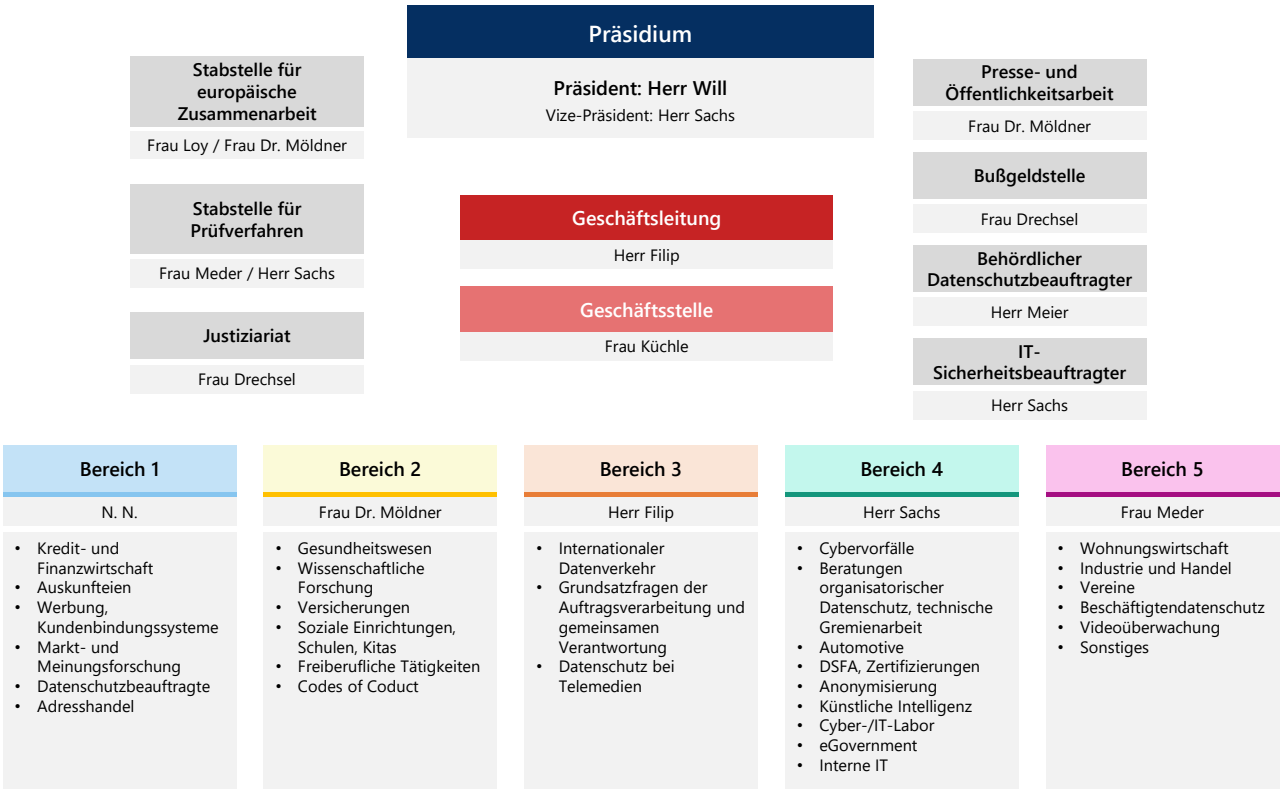
als gleichwertige und gleichrangige Aufsichtsbehörden im Sinne des Art. 51 DS-GVO gesetzlich festgelegt. Vor dem Hintergrund der gemeinsamen Verpflichtung zur einheitlichen Anwendung und Durchsetzung der DS-GVO enthält Art. 21 BayDSG klarstellend einen an alle vier Behörden adressierten Auftrag zur gegenseitigen Zusammenarbeit und Unterstützung. Im aufsichtlichen Alltag wird diesem Auftrag durch einen stetigen Informationsaustausch vor allem in Querschnittsbereichen wie dem Gesundheitswesen oder dem Internetrecht und regelmäßige Positionsabstimmungen insbesondere mit dem Bayerischen Landesbeauftragten für den Datenschutz und dem Medienbeauftragten für den Datenschutz für die Bayerische Landeszentrale für neue Medien Rechnung getragen.

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

1.3 Das Bayerische Landesamt für Datenschutzaufsicht

Fallzahlen nahezu auf dem Spitzenniveau der Vorjahre lassen ahnen, dass auch das Jahr 2022 alle Bereiche des Landesamts Woche für Woche vor enorme Herausforderungen gestellt hat, um den vielfältigen Aufgaben der Datenschutzaufsicht letztlich gerecht zu werden. Auch im fünften Jahr ihrer Geltung ist in jedem der fünf Fachbereiche nach wie vor spürbar, dass die DS-GVO unsere bisherigen Arbeitsbedingungen verändert und uns mit der Aufgabe der Zusammenarbeit mit den anderen Aufsichtsbehörden der Mitgliedsstaaten neue Handlungsformen, Abläufe und letztlich auch Organisationsstrukturen abverlangt.

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 2022 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 2022 bei uns eingegangen sind, ist der unten folgenden Grafik zu entnehmen. Sie zeigt einen Rückgang um 16 % im Vergleich zu 2021. Eine genauere Betrachtung vermittelt folgende Befunde:

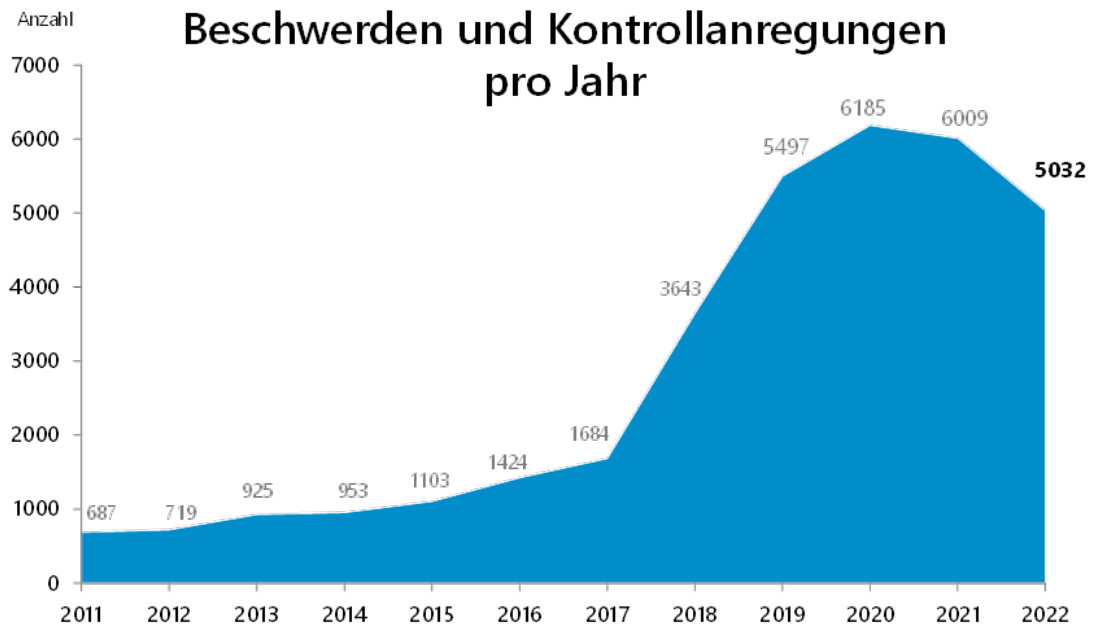
Beschwerden im Bereich Internet (Tracking, Einwilligungsbanner, Datenschutzerklärungen) nehmen wie die letzten Jahre die zahlenmäßig umfangreichste Position ein. Dennoch ging die Gesamtzahl der Vorgänge deutlich von 2021 zu 2022 um 35 % zurück.

Auf Platz zwei folgen dicht Beschwerden im Bereich Videoüberwachung, die sich sogar mit einem Zugang von 7 % gegen den Trend stellten.

Eine Zunahme der Beschwerden verzeichnete ebenfalls der Bereich des internationalen Datenverkehrs, dessen Fallbelastung in 2022 (von einem mittleren zweistelligen absoluten Niveau) damit sogar um 170 % zunahmen.

Die restlichen Beschwerdebereiche wie Finanzen, Gesundheit, Versicherung, Handel, etc. haben isoliert betrachtet um 9 % abgenommen, Beschwerden im Bereich technischer Datenschutz sind mit einer Abnahme von 5 % fast gleichgeblieben.

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



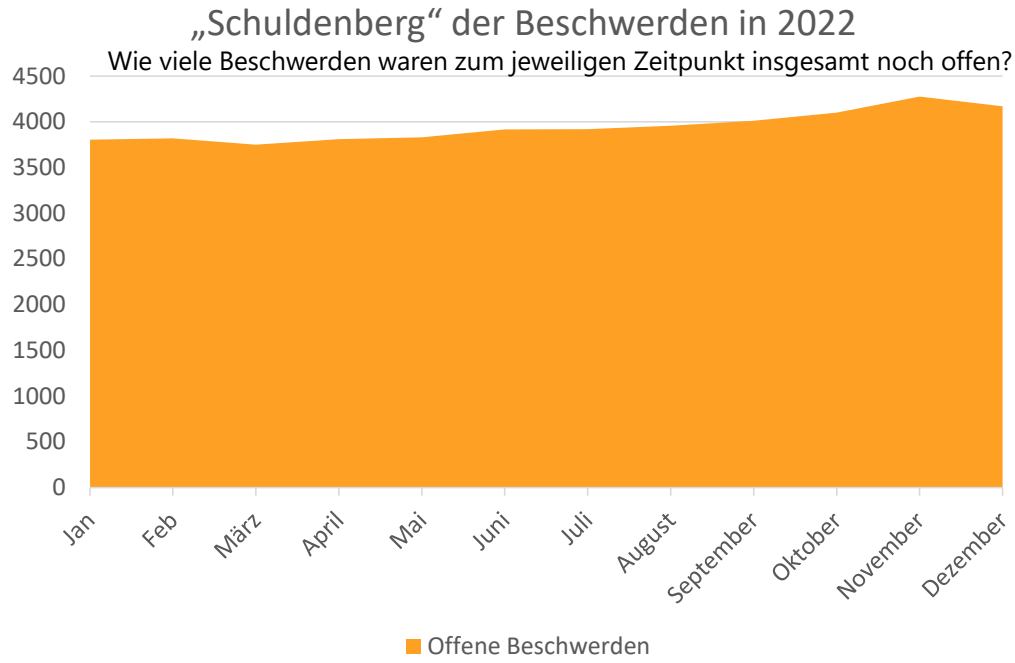
Unter dem Obergriff „Beschwerden“ erhielten wir auch im Jahr 2022 mit einem Prozentsatz von 29 % eine erhebliche Anzahl von Meldungen über Datenschutzverstöße, bei denen die Eingabeführer:innen nicht glaubhaft gemacht haben, durch den vorgetragenen Sachverhalt in den eigenen Rechten verletzt zu sein. Diese Eingänge bezeichnen wir nicht als Beschwerden, sondern als Kontrollanregungen.

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

Kann die Aufsichtsbehörde dieser Verpflichtung nicht nachkommen, steht dem Betroffenen eine (Untätigkeits-)Klage offen. Zu berücksichtigen bleibt freilich, dass im Wege der Untätigkeitsklage lediglich die gerichtliche Feststellung erreicht werden kann, dass die Aufsichtsbehörde zur umgehenden Prüfung des Beschwerdevorbringens verpflichtet ist, regelmäßig nicht aber eine Sachentscheidung z. B. in Gestalt einer Untersagung der strittigen Datenverarbeitung. Im allseitigen Interesse an der Vermeidung solch eigentlich unproduktiver Streitigkeiten sind wir daher trotz aller Fallbelastungen vorrangig bestrebt, den Zielwert der Drei-Monatsfrist des Art. 78 Abs. 2 DS-GVO nicht zu verfehlen. Dies ist uns in 2022 aufgrund unzureichender Ressourcen nur bei rund 60% der Beschwerden gelungen.

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

Der Rückgang der Gesamt-Beschwerdezahlen in 2022 beruht zusammenfassend vor allem darauf, dass sich gerade im Bereich des Internets die Fallzahlen von einem sehr hohen zu einem hohen Niveau verschoben haben, was mit zunehmender Umsetzung datenschutzrechtlicher Anforderungen des TTDSG bei Verantwortli-



chen insbesondere im Bereich Einwilligungsbanner erklärt werden kann. Die Reduzierung um durchschnittlich 9 % scheint einerseits den allgemeinen Trend zu geringeren Beschwerdezahlen bei einigen deutschen Datenschutzaufsichtsbehörden widerzuspiegeln. Dies ist im besten Fall ein Beleg dafür ist, dass im Jahr vier (2022) der Datenschutzgrundverordnung die Mehrzahl der Verantwortlichen einen zunehmend stabilen Reifegrad bei deren DS-GVO Umsetzung erreicht haben. Andererseits weist der Anstieg im Bereich der Videoüberwachung auf eine weniger positive Ursache rückläufiger Beschwerdezahlen hin: Videoüberwachung unterscheidet sich auch deshalb von anderen Verarbeitungen personenbezogener Daten, da die Kameras gesehen und die Rechte der Betroffenen naheliegender eingefordert werden können als bspw. bei der Speicherung von Persönlichkeitsprofilen in internen Unternehmensdatenbanken. Durch die zunehmende Digitalisierung von Geschäftsprozessen verschwinden Datenverarbeitungen aus dem unmittelbaren Blickwinkel der Betroffenen, zeitgleich nehmen die Risiken für diese aufgrund möglicher weltweiter Datenflüsse bei der Nutzung von Cloud-Diensten oder zunehmend komplexen Verarbeitung wie durch KI-Systeme zu. Deswegen gibt die Verringerung der Beschwerdezahlen bei genauer Betrachtung eher keinen Anlass dafür, von einer „Entwarnung“ zu sprechen. Sie muss vielmehr als Warnsignal verstanden werden, das zunehmend den Bedarf für anlasslose Datenschutzkontrollen bei bayerischen Unternehmen aufzeigt.

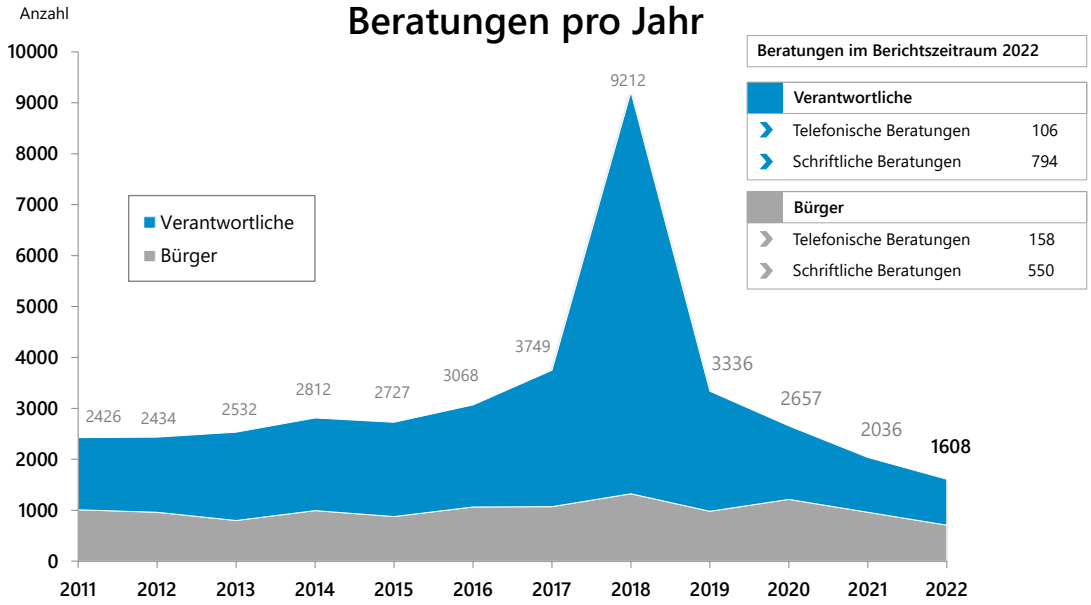
Der Blick auf unsere Bearbeitungsrückstände („Schuldenberg“) in 2022 zeigt trotz gesunkener Beschwerdezahlen weiterhin leichte Anstiege. Vordergründig könnte diese Entwicklung schon mitpersonellen Sondereffekten wie familiär bedingten Auszeiten oder Arbeitszeit-verkürzungen mehrerer Mitarbeiter:innen begründet werden., die sich bei einer kleinen Behörde wie dem BayLDA unmittelbar und unvermeidbar in Produktivitätseinbußen niederschlagen. Genauer analysiert ist aber auch festzustellen, dass die Bearbeitung von Beschwerdevorgängen zunehmend zeitaufwändiger wird Die Anzahl der Sachverhalte, die fast schematisch quasi unmittelbar nach Erstsichtung bewertet und dadurch unverzüglich abgeschlossen werden konnten, wird bereichsübergreifend zunehmend geringer - trotz aller sonst erfolgreichen Bemühungen um Effizienz und Teilautomatisierung durch unser eGovernment-Verfahren IGOR. Dies führt zwangsläufig zu längeren Bearbeitungszeiten, da Abstriche an der Qualität unserer datenschutzrechtlichen Prüfung aus gutem Gründen nicht statthaft wären.

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 ist die Anzahl der Beratungen im Verhältnis zum Vorjahr weiter gesunken.

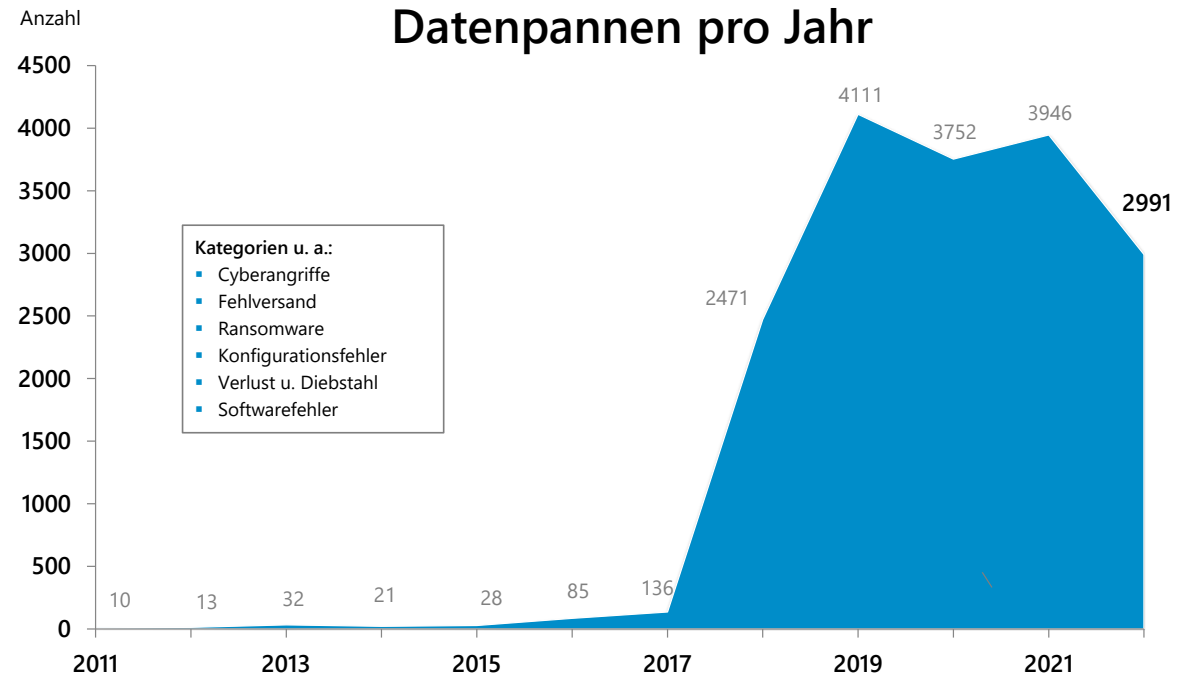
Damit hat sich unserer Einschätzung aus dem Vorjahr be- und verstetigt, dass unsere Ressourcenlage kaum mehr eine rechtzeitige und bedarfsgerechte Beratung von datenschutzrechtlichen Anliegen zulässt. Die Zahl von 1608 Beratungsanfragen in 2022 stellt einen neuen Tiefstand in der Geschichte des BayLDA dar.



Angesichts unzureichender Ressourcen unterliegen für Beratungsanliegen einer klaren Priorisierung: Dies bedeutet, dass spezifische 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

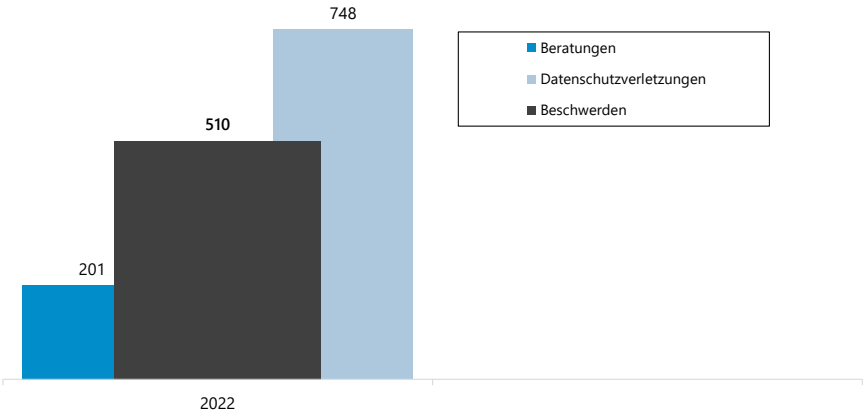
Anders als in den vorangegangenen Jahren ist die Zahl der Meldungen von Verletzungen der Sicherheit bei der Verarbeitung personenbezogener Daten in 2022 deutlich auf 2991 gesunken. Datenschutzverletzungen bestimmten in 2022 neben den Beschwerden aber dennoch weiterhin unseren Arbeitsalltag, der fast die kompletten Ressourcen des Bereichs 4 „Cybersicherheit und technischer Datenschutz" beanspruchten.



In der oben aufgeführten Grafik werden die bei uns eingegangenen Meldungen nach Art. 33 DS-GVO dargestellt. Weitere Informationen zum Thema Datenschutzverletzungen, insbesondere zur Interpretation der Fallzahlen im Allgemeinen sind im Kapitel 14 Cybersicherheitslage dieses Berichts zu finden.

2.4 Ressourcen

Im Berichtszeitraum konnte das BayLDA auf Grund der zeitlich aufwändigen Teilnahme in der Cyberabwehr Bayern zumindest vorläufig eine zusätzliche Informatikerstelle durch Zuweisungen des Bayerischen Innenministeriums gewinnen. Unsere Stellenanmeldung für den Einjahreshaushalt 2022 fanden dagegen, wie bereits in der Einleitung dargestellt, keine Berücksichtigung. Auf Grundlage dieser Stellensituation ergibt sich das in der dargestellten Grafik aufgezeigte Verhältnis zwischen Fallzahlen und konkret eingesetzten Mitarbeiter:innenstellen. So bearbeitet bspw. eine Sachbearbeiter-Planstelle des Bereich 4 rechnerisch pro Jahr im Durchschnitt 748 Meldungen zu den Verletzungen der Sicherheit nach Art. 33 DSGVO. Auch die Anzahl von 510 Beschwerden pro Sachbearbeiter-Planstelle im Bereich Beschwerdebearbeitung liegt auf einem äußerst hohen Niveau.



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

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

Die Gesamtzahl aller von Deutschland initiierten IMI-Verfahren lag im Jahr 2022 bei 2891, davon wurden ca. 16 % vom BayLDA in die Wege geleitet. Nur Berlin hat damit mehr grenzüberschreitende Sachverhalte in Bearbeitung (rund

36 % der deutschen IMI-Verfahren). Angesichts dessen, dass Deutschland insgesamt auf Platz 2 nach Irland liegt mit 21% aller IMI-Verfahren (Irland: 25%), sind diese Fallzahlen zwar auf Grund der wirtschaftlichen Struktur des Freistaates mit dem deutschlandweiten Hauptsitz zahlreicher europaweit agierender Unternehmen nachvollziehbar. Für eine deutschlandweit unterdurchschnittlich ausgestattete Behörde bleiben sie dennoch eine Herausforderung.

Bei rund 12 % der Verfahren war das LDA 2022 federführende Aufsichtsbehörde, was uns nach unserer Rechnung auf Platz 3 nach Berlin und BfDI befördert. Diese Rechnung ergibt sich daraus, dass wir in der Regel bei den Verfahren nach Art. 61 DS-GVO, die wir eröffnet haben, auch federführende Aufsichtsbehörde sind.

In weiteren 70 % der Verfahren, bei denen eine oder mehrere deutsche Aufsichtsbehörden gegenseitige Amtshilfe gemäß Art. 61 DS-GVO leisteten, waren wir betroffene Aufsichtsbehörde und belegen damit hier Platz 1 innerhalb Deutschlands.

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

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

3.2 Mitwirkung in Subgroups des EDSA

Der Europäische Datenschutzausschuss (EDSA) dient der Sicherstellung einer europaweit einheitlichen Anwendung der Datenschutz-Grundverordnung (vgl. Art. 70 Abs. 1 Satz 1 DS-GVO). Er besteht aus dem/der Leiter:in einer Aufsichtsbehörde jedes Mitgliedstaates und dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertreter:innen (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 ein/e Vertreter:in des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) sowie ein/e Vertreter:in einer Aufsichtsbehörde eines Landes sowie eines/r stellvertretenden Landesvertreter:in. Hierbei sollen die von der DSK ernannten Vertreter:innen Deutschland als Ganzes repräsentieren und nicht (nur) die eigene Behörde.

Im Berichtszeitraum stellten wir weiterhin den Landesvertreter in der International Transfer Expert Subgroup und seit Ende 2022 zudem eine Landesvertreterin für die Compliance, eGovernance and Health Subgroup. Unsere Rolle als stellvertretende Landesvertreterin für die Cooperation Expert Subgroup mussten wir im Jahresverlauf dagegen aus Kapazitätsgründen aufgeben. 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, zu BcR-Formularen oder zur 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 ein nicht anders als die Erfüllung der Rechte von Beschwerdeführern eine Pflichtaufgabe aufsichtlichen Handelns, wie Art. 51 Abs. 2 DS-GVO unterstreicht.

4

Allgemeines / Betroffenenrechte

4 Allgemeines / Betroffenenrechte

4.1 Reichweite der Haushaltsausnahme gem. Art. 2 Abs. 2 Buchst. c DS-GVO

Die DS-GVO ist auch bei Datenverarbeitungen durch Privatpersonen anwendbar.

Immer wieder erreichen uns Beratungsanfragen und Beschwerden, in denen es zunächst darum geht, zu bewerten, ob die DS-GVO überhaupt auf die Verarbeitung von personenbezogenen Daten Anwendung findet oder ob die Verarbeitung zur Ausübung ausschließlich persönlicher oder familiäre Tätigkeiten (vgl. Art. 2 Abs. 2 Buchst. c DS-GVO) erfolgt.

Konkret stellt sich die Frage immer dann, wenn eine Privatperson personenbezogene Daten verarbeitet und diese Daten dabei die eigene private Sphäre verlassen. Eindeutig als unter den Anwendungsbereich des Datenschutzrechts fallend sehen wir insbesondere die Fälle, in denen personenbezogene Daten z.B. im Internet der Öffentlichkeit allgemein zugänglich gemacht werden. Dies ist regelmäßig vor allem auch bei Veröffentlichungen in sozialen Netzwerken anzunehmen, wenn Privatpersonen beispielweise auf ihren Profilseiten Beiträge erstellen, da diese meist einem Personenkreis zugänglich sind, der über den persönlichen und familiären Kreis hinausgeht. Insbesondere durch die Möglichkeit, Beiträge zu teilen, kann nicht sichergestellt werden, ob eine Veröffentlichung auf den persönlichen Bereich beschränkt bleibt. Ausschlaggebend ist zudem, ob die Veröffentlichung für einen begrenzten Personenkreis - welcher dem persönlichen und familiären Kreis zuzurechnen ist - erfolgt oder jedermann zugänglich ist. Bei einem Facebook-Account mit 20 Freund:innen die der/dem Accountinhaber:in bekannt sind, wird dies im Regelfall unter die Haushaltsausnahme zu fassen sein. Schwieriger ist die Abgrenzung dagegen bei zwar eingeschränkt einsehbaren Profilen, welche jedoch beispielsweise 500 „Freund:innen“ haben, die die Veröffentlichung wahrnehmen können.

Ein weiteres Beispiel, welches uns in der aufsichtlichen Praxis häufig begegnet, ist die Weitergabe von personenbezogenen Daten in WhatsApp-Gruppen. Auch hier gilt es zu prüfen, wer die Empfänger:innen sind und ob diese dem persönlichen und familiären Bereich zugerechnet werden können. Die Nachrichten in einer Klasseneltern-Gruppe kann man in der Regel der Haushaltsausnahme zuordnen. Sofern aber beispielsweise Lehrkräfte Zugriff auf die Inhalte haben, ist dies weniger eindeutig. In einem konkreten Fall haben wir den Anwendungsbereich der DS-GVO als eröffnet angesehen, da Nachrichten aus einer solchen WhatsApp-Gruppe ausgedruckt und der Schulleitung vorgelegt worden sind.

Weniger eindeutig sind Fallgestaltungen, in denen personenbezogene Daten im Rahmen einer Anzeige an Ermittlungsbehörden oder sonstige öffentliche Stellen (wie z.B. Jugendamt, Gewerbeaufsicht, Zoll) weitergegeben werden.

In unseren „Falschparker-Fotografen“-Verfahren vertraten wir die Auffassung, dass die Weitergabe von Fotos, die von verkehrswidrig parkenden Kraftfahrzeugen angefertigt wurden und das Kfz-Kennzeichen erkennen ließen, und die zum Zwecke der Anzeige angefertigt wurden in den Anwendungsbereich des Datenschutzrechts fallen. Dies wurde durch das Bayerische Verwaltungsgericht Ansbach bestätigt (vgl. Urteile des VG Ansbach vom 02.11.2022, AN 14 K 22.00468 und AN 14 K 21.01431).

4.2 Wann liegt eine Beschwerde bei der Aufsichtsbehörde vor?

Die Aufsichtsbehörde kann eine Eingabe nur dann als Beschwerde im gesetzlichen

Sinne behandeln, wenn darin der Beschwerdegegner sowie der Verantwortliche genannt wird, der Sachverhalt in ausreichend konkretisierter Form beschrieben ist und erkennbar ist, wogegen sich die Eingabe führende Person wendet, d.h. in welchen Aspekt bzw. welchen Aspekten des Sachverhalts sie mögliche datenschutzrechtliche Verstöße sieht.

Jede betroffene Person kann sich nach Art. 77 DS-GVO an eine der für den Vollzug der DS-GVO zuständigen Datenschutzaufsichtsbehörden wenden, wenn sie der Ansicht ist, dass eine Verarbeitung von sie betreffenden personenbezogenen Daten gegen die DS-GVO verstößt.

Auch im Lichte dieses vom Gesetzgeber bewusst niederschwellig gestalteten Zugangs zur Aufsichtsbehörde müssen Eingaben an die Aufsichtsbehörde gewisse inhaltliche Mindestanforderungen erfüllen, um als Beschwerde im Sinne von Art. 77 DS-GVO eingestuft werden und so die in Artikel 57 Abs. 1 Buchst. f DS-GVO geregelte Pflicht der Aufsichtsbehörde zur Befassung mit einer Beschwerde sowie zur Untersuchung des Beschwerdegegenstands auslösen zu können. Insbesondere muss ein:e Beschwerdeführer:in den Lebenssachverhalt, im Rahmen dessen seine/ihre personenbezogenen Daten verarbeitet wurden und den behaupteten Verstoß so ausreichend konkretisiert beschreiben, dass die Aufsichtsbehörde diesen möglichst ohne weitere Rückfragen verstehen und ihn entweder schon unmittelbar datenschutzrechtlich bewerten kann oder aber zumindest den/die Beschwerdegegner:in (d.h. einen Verantwortlichen oder Auftragsverarbeiter) mit dem dergestalt umschriebenen Sachverhalt konfrontieren und ihn, sofern für die Untersuchung nötig, um Bereitstellung etwaiger weiterer Informationen ersuchen kann (vgl. Art. 57 Abs. 1 Buchst. a DS-GVO). Vor einer abschließenden Bewertung ist dem/der Beschwerdegegner:in ohnehin – außer bei vollständiger Zurückweisung der Beschwerde - schon aus verfahrensrechtlichen Gründen stets Gelegenheit zur Stellungnahme zu geben.

Auf unserem Online-Beschwerdeportal informieren wir Personen, die die Einlegung einer Beschwerde erwägen, mit Blick auf den von ihnen anzugebenden „Sachverhalt der Beschwerde“ wie folgt:

„Bitte beschreiben Sie Ihren Beschwerdesachverhalt möglichst präzise – welche Daten sind unrichtig verarbeitet worden? Wann? Von wem? Auf welche Weise? Was haben Sie zwischenzeitlich unternommen? Wie haben die angesprochenen Stellen reagiert? Welche Dritte haben Kenntnis von den Daten durch den Vorfall erlangt bzw. hatten die Möglichkeit zur Kenntnisnahme?“.

Die hier zitierten Fragen sind zwar in letzter Konsequenz nur im Sinne von Beispielen zu verstehen, umschreiben aber doch für die Mehrzahl der Fälle diejenigen Angaben, die typischerweise notwendig sind, damit die Aufsichtsbehörde den der Beschwerde zugrunde liegenden Lebenssachverhalt ausreichend einordnen und nachvollziehen sowie erkennen kann, gegen welche(n) Aspekt(e) der dabei in Rede stehenden Verarbeitung ihrer personenbezogenen Daten sich die beschwerdeführende Person wendet, d.h. worin genau sie einen (möglichen) datenschutzrechtlichen Verstoß sieht.

In der aufsichtlichen Praxis erreichen uns immer wieder auch Eingaben, die diese Mindestanforderungen – zumindest anfänglich – nicht erfüllen, so dass uns auf Basis des ersten Eingangs noch nicht möglich ist, in eine Untersuchung einzusteigen. So fehlen zum Teil ausreichende Angaben zur Identität des Beschwerdegegners, oder der Sachverhalt wird nur sehr allgemein umschrieben. Bisweilen lässt sich einer Eingabe nicht ausreichend entnehmen, um welchen Lebenssachverhalt es überhaupt geht, d.h. insbe-

sondere in was für einer Situation bzw. vor welchem Hintergrund überhaupt personenbezogene Daten der betroffenen Person verarbeitet wurden, in welcher Form und/oder zu welchem Zweck die Verarbeitung erfolgte und/oder um welche Daten es geht. Manche Eingaben bestehen lediglich aus knappen plakativ-bewertenden Aussagen etwa des Typs, dass der Verantwortliche (nicht näher bezeichnete) „Daten weitergegeben" habe, und zwar „ohne Einwilligung" o.ä., ohne jedoch den Lebenszusammenhang der erwähnten Datenweitergabe zu beschreiben. Gelegentlich wird zwar von „Datenweitergabe" gesprochen, ohne dass jedoch mitgeteilt wird, an wen die Daten (bzw. welche Daten eigentlich) weitergegeben wurden. Immer wieder werden uns außerdem Sachverhalte so geschildert, dass für uns der Beschwerdegegenstand nicht erkennbar ist. In solchen und anderen Fällen mit unvollständiger Sachverhaltsbeschreibung wenden wir uns mit möglichst gezielten Rückfragen an die beschwerdeführende Person und bitten unter Setzung einer angemessenen Frist um Nachreichung der aus unserer Sicht für die Bearbeitung benötigten Informationen. Hierbei informieren wir die Beschwerde führende Person, dass wir, sofern uns diese Informationen nicht binnen der Frist nachgereicht werden, die Eingabe nicht als Beschwerde bearbeiten können und den Vorgang daher nach Fristablauf ohne nochmalige Nachricht abschließen werden.

Keine Beschwerde im Sinne von Art. 77 DS-GVO liegt ferner dann vor, wenn der in einer Eingabe dargestellte Sachverhalt zwar die Verarbeitung personenbezogener Daten zum Gegenstand hat, es sich jedoch nicht um Daten des/der Eingabeführer:in handelt, sondern um Daten, die sich auf andere Personen beziehen. Dennoch haben die Datenschutzaufsichtsbehörden auch in solchen Fällen die Möglichkeit, den dargelegten potentiellen Verstoß aufsichtlich zu überprüfen. Die Prüfung erfolgt in solchen Fällen nicht im Wege eines Beschwerdeverfahrens, sondern in einem von Amts wegen geführten Verfahren. Da es sich in solchen Fällen bei der Person, die die Eingabe eingereicht hat, nicht um eine „betroffene Person" im Sinne von Art. 4 Nr. 1 DS-GVO und beim Verfahren nicht um ein Beschwerdeverfahren handelt, kommen die Artikel 77 und 78 der DS-GVO nicht zur Anwendung, so dass die die Eingabe führende Person anders als für Beschwerden in Art. 77 Abs. 2 DS-GVO vorgesehen von der Aufsichtsbehörde keine weitere Nachricht über den Stand und das Ergebnis der aufsichtlichen Untersuchung erhält.

In einem konkreten Fall wurde uns eine E-Mail zugesandt, bei der wir neben zwei Unternehmen in das „An"-Feld der E-Mail gesetzt worden waren. Die E-Mail selbst begann mit der Anrede „Sehr geehrte Damen und Herren bei (hier wurden die zwei Namen der zwei Unternehmen genannt) …". Das Bayerische Landesamt für Datenschutzaufsicht wurde weder in der Anrede noch im weiteren Inhalt der E-Mail direkt angesprochen, vielmehr wurden in der E-Mail nur die beiden Unternehmen mehrfach direkt mit „Sie" angesprochen. Der Sache nach beschwerte sich der Absender (und spätere Kläger) im Wesentlichen über die Verwendung von Cookies durch die genannten Unternehmen, ohne jedoch konkrete URLs von Websites anzugeben, auf die sich seine Schilderung bezog. Kurz vor Ende der Mail hieß es: „Der Einfachheit halber (…) sende ich dieses Schreiben zeitgleich auch an die zuständige Datenschutzaufsichtsbehörde." In diesem Fall schrieben wir an die absendende Person, dass wir die Mail nicht als Beschwerde im Sinne von Art. 77 DS-GVO bewerten, weil der Inhalt der Mail nicht erkennen ließ, dass der Absender sein Anliegen unmittelbar an uns gerichtet habe. Zudem teilten wir mit, dass die E-Mail den Sachverhalt und den angenommenen datenschutzrechtlichen Verstoß nicht ausreichend umschreibe, und wir den Vorgang daher nur dann als Beschwerde bearbeiten können, wenn ausreichend konkretisierte Informationen zum Sachverhalt nachgeliefert würden, insbesondere die URLs, auf die sich der Absender beziehen möchte. In der Folge entwickelte sich zwischen uns und dem Absender ein E-Mail-Verkehr, im

Rahmen dessen jedoch der Absender keine weiteren inhaltlichen Angaben zum Sachverhalt machte und insbesondere keine URLs der Internetseiten mitteilte, auf die er seine Eingabe bezogen wissen wollte.

Wir wiederholten daraufhin, dass mangels ausreichender Angaben zum Sachverhalt -insbesondere zu den URLs oder ggf. den Apps, um die es dem Absender gehe – auch weiterhin keine Beschwerde im Sinne von Art. 77 DS-GVO vorliege. Ohne anschließend weitere Angaben zum Sachverhalt gemacht zu haben erhob der Absender der E-Mails einige Zeit später Untätigkeitsklage gegen uns beim Verwaltungsgericht Ansbach. Das Verwaltungsgericht entschied mit inzwischen rechtskräftigem Urteil, dass der Kläger keine wirksame Beschwerde im Sinne von Art. 77 DS-GVO eingelegt hatte, weil für einen objektiven Dritten aus der E-Mail nicht erkennbar war, dass der Absender damit die Einleitung eines Beschwerdeverfahrens bei der Aufsichtsbehörde herbeiführen wollte. Stattdessen sei die E-Mail bei objektiver Betrachtung im Sinne eines Hinweises an die darin angesprochenen Unternehmen zu verstehen oder aber als Wunsch auf Einbeziehung unseres Hauses in eine weitergehende, künftige Korrespondenz zwischen dem (späteren) Kläger und den angesprochenen Unternehmen. Erhebliches Gewicht kam dabei nach Ansicht des Verwaltungsgerichts – neben weiteren Gesichtspunkten - dem Umstand zu, dass unser Haus selbst in der gesamten E-Mail vom Absender an keiner Stelle direkt angesprochen worden war. Daher sei es in dieser ersten E-Mail nicht erkennbar gewesen, dass der Absender mit der E-Mail eine Rechtsfolge beim Bayerischen Landesamt für Datenschutzaufsicht herbeiführen wollte. Dass der Mail-Absender und spätere Kläger im Betreff-Feld der Mail den Begriff „Beschwerde“ verwendet hatte, führte nach Auffassung des Gerichts zu keinem anderen Ergebnis, ebenso wenig wie der Umstand für sich gesehen, dass das BayLDA die E-Mail im „An“-Feld und nicht lediglich im „cc“-Feld erhalten hatte. In seinen weiteren E-Mails an uns habe der spätere Kläger dann zwar seinen Willen zur Einreichung einer Beschwerde artikuliert, hatte jedoch trotz entsprechenden Hinweises auch weiterhin nicht die von uns spezifizierten weiteren Informationen zum Sachverhalt nachgereicht, insbesondere nicht die URLs der Websites genannt, deren Überprüfung er anstrebte. Vor diesem Hintergrund bestätigte das Gericht, dass der spätere Kläger dem BayLDA nicht die Mindestinformationen zur Verfügung gestellt hatte, die notwendig gewesen wären, um den Sachverhalt ausreichend zu umschreiben und den Beschwerdegegner zu spezifizieren. Nach Ansicht des Gerichts war schon nicht erkennbar, gegen welchen Webseitenbetreiber sich die Beschwerde richten soll, dies insbesondere vor dem Hintergrund, dass beide vom E-Mail-Absender genannten Unternehmen jeweils mehrere Webseiten betreiben. Das Gericht bestätigte im Ergebnis, dass es mangels dieser Mindestinformationen für das Bayerischen Landesamt für Datenschutzaufsicht nicht möglich war, ein Beschwerdeverfahren einzuleiten. Letztlich hatte der spätere Kläger aus Sicht des Verwaltungsgerichts somit keine wirksame Beschwerde nach Art. 77 DS-GVO bei uns eingelegt.

4.3 Keine (ausreichende/fristgerechte) Reaktion auf Auskunftsersuchen gem. Art. 15 DS-GVO

Auskünfte gem. Art. 15 DS-GVO sind grundsätzlich vollständig binnen Monatsfrist zu erteilen.

Stellt eine betroffene Person ein Auskunftsersuchen gem. Art. 15 DS-GVO, so sieht Art. 12 Abs. 3 DS-GVO grundsätzlich vor, dass die Auskunft seitens des Verantwortlichen unverzüglich, jedenfalls aber binnen Monatsfrist erteilt wird. Die Monatsfrist beginnt an dem Tag, an dem das Auskunftsersuchen bei dem Verantwortlichen einging. Soweit die Identität ungewiss ist und bestätigt werden muss (vgl. Art. 12 Abs. 6 DS-GVO), beginnt die Frist an dem Tag, an dem der

Verantwortliche, der unverzüglich die erforderlichen Informationen erfragt hat, Gewissheit über die Identität des/der Auskunftsersuchenden hat. Fällt das Fristende auf einen Samstag, Sonntag oder Feiertag, so endet diese mit Ablauf des nächsten Werktages (vgl. hierzu die Leitlinien des EDSA 01/2022 zum Auskunftsrecht, Rn. 157 ff.).

Im Berichtszeitraum haben wir zahlreiche Eingaben erhalten, bei denen eine Reaktion auf ein Auskunftsersuchen entweder vollständig ausblieb, lediglich eine Eingangsbestätigung versandt wurde, die Monatsfrist entgegen Art. 12 Abs. 3 S. 3 DS-GVO ohne weitere Begründung verlängert wurde oder die Auskunft unvollständig war.

Zu einem Überschreiten der Monatsfrist des Art. 12 Abs. 3 DS-GVO kam es dabei zum Teil deshalb, weil das Auskunftsersuchen durch die betroffene Person nicht direkt an den Verantwortlichen, sondern zunächst an einen Auftragsverarbeiter gerichtet wurde und eine unverzügliche Weiterleitung nicht erfolgte. Dabei ist in einem Auftragsverarbeitungsvertrag gem. Art. 28 Abs. 3 Buchst. e DS-GVO insbesondere auch vorzusehen, dass der Verantwortliche nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützt wird, seiner Pflicht zur Beantwortung von Ersuchen gem. Art. 12 ff. DS-GVO, somit auch eines Auskunftsersuchens nachzukommen. Auch wenn keine konkreten Bestimmungen zum Vorgehen im Zusammenhang mit Betroffenenrechten im Auftragsverarbeitungsvertrag enthalten sind, sehen wir es jedenfalls als möglich und zumutbar an, dass z.B. Auskunftsersuchen bezüglich der im Auftrag verarbeiteten personenbezogenen Daten unverzüglich an den Verantwortlichen weitergeleitet werden, so dass diesem eine fristgerechte Reaktion möglich ist. Geht also das Ersuchen beim Auftragsverarbeiter ein, bewirkt dies den Fristbeginn beim Verantwortlichen, nachdem diesen das Handeln des Auftragsverarbeiters insoweit zuzurechnen ist. Dieser handelt auch hier als verlängerter Arm des Verantwortlichen. In den uns vorliegenden Konstellationen wurden durch den Auftragsverarbeiter keine personenbezogenen Daten der betroffenen Personen in eigener Verantwortung verarbeitet, so dass diesbezüglich zudem ein Negativattest hinsichtlich einer eigenen Datenverarbeitung abzugeben war.

Die häufigsten Fälle, in denen keine vollständige Auskunft erteilt wurde, betrafen entweder Fälle, in denen die Informationen gem. Art. 15 Abs. 1 Buchst. a bis h, Abs. 2 DS-GVO nicht erteilt wurden, sondern eine pauschale Beauskunftung nur der gespeicherten Stammdaten erfolgten ohne auf die weiteren geforderten Informationen einzugehen. Darüber hinaus wurden häufig nur Kategorien der personenbezogenen Daten und/oder Kategorien von Empfängern benannt, ohne dass die konkreten personenbezogenen Daten gem. Art. 4 Nr. 1 DS-GVO bzw. die konkreten Empfänger gem. Art. 4 Nr. 9 DS-GVO benannt wurden. Nach Sinn und Zweck des Auskunftsrechtes ist es jedoch erforderlich, dass die betroffene Person gerade die konkreten Informationen erhält, um sich der Verarbeitung bewusst zu sein, die Rechtmäßigkeit der Datenverarbeitung und die Richtigkeit der verarbeiteten Daten überprüfen zu können (vgl. Erwägungsgrund 63). Dass grundsätzlich die konkrete Identität der Empfänger zu beauskunften ist, hat zwischenzeitlich auch der EuGH (Urteil vom 12.01.2023, C- 154/21) bestätigt. Nach dem Sinn und Zweck des Auskunftsrechts ist es darüber hinaus erforderlich, dass der Verantwortliche darüber Auskunft gibt, welche konkreten personenbezogenen Daten an welchen konkreten Empfänger gingen. Nur so ist es der betroffenen Person möglich, zu erfahren, welche personenbezogenen Daten an welchem Empfänger weitergegeben wurden und die Rechtmäßigkeit der Datenverarbeitung zu überprüfen. Die Möglichkeit, bei dem benannten Empfänger (soweit es sich um einen Verantwortlichen gem. Art. 4 Nr. 7 DS-GVO handelt) wiederum ein Auskunftsersuchen zu stellen, entbindet den Verantwortlichen nicht von dieser Pflicht, da der Betroffene

ja gerade die Rechtmäßigkeit der Verarbeitung des jeweiligen Verantwortlichen überprüfen können soll.

4.4 Umfang des Auskunftsanspruchs

Kopie der verarbeiteten personenbezogenen Daten bedeutet nicht die Vervielfältigung und Herausgabe aller vorhandenen Schriftstücke.

Unter Bezugnahme auf die Formulierung in Art. 15 Abs. 3 DS-GVO erreichten uns zahlreiche Anfragen und Eingaben dazu, inwieweit Schriftverkehr (insbesondere postalische Schreiben und E-Mails), Notizen und sonstige Dokumente im Rahmen einer Beauskunftung durch den Verantwortlichen herauszugeben, d.h. ein Duplikat dieser Dokumente zur Verfügung zu stellen sind.

Hierzu teilten wir mit, dass Art. 15 Abs. 3 DS-GVO den Verantwortlichen dazu verpflichtet, der auskunftsersuchenden Person eine „Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind" zur Verfügung zu stellen. Dies bedeutet gerade nicht, dass Originaldokumente fotokopiert und zur Verfügung gestellt werden müssen, sondern dass die personenbezogenen Daten mitsamt den Informationen gem. Art. 15 Abs. 1 und Abs. 2 DS-GVO zu beauskunften sind. Diese Zusammenstellung muss es der betroffenen Person ermöglichen, Kenntnis von ihren Daten zu erhalten und die Richtigkeit und Rechtmäßigkeit der verarbeiteten personenbezogenen Daten überprüfen zu können. Sind somit die einzelnen Schriftstücke o.ä. nicht per se als personenbezogenes Datum i.S.d. Art. 4 Nr. 1 DS-GVO einzustufen und ist ein Schriftstück bzw. Auszüge hiervon nicht notwendig, um den Kontext, in dem die Datenverarbeitung stattfand, zu verstehen, so sind – vorbehaltlich der Einschränkungen des Auskunftsrechts (z.B. gem. Art. 15 Abs. 4 DS-GVO) - alleine die personenbezogenen Daten, die in dem entsprechenden Schriftstück enthalten sind sowie die zugehörigen Informationen gem. Art. 15 Abs. 1 Buchst. a bis h, Abs. 2 DS-GVO zu beauskunften. Diese Ansicht wird auch durch das zwischenzeitlich ergangene Urteil des EuGH vom 4. Mai 2023, C-487/21 bestätigt.

Möchte der Verantwortliche dem Auskunftsersuchenden von vornherein alle Schriftstücke in Originalform, d.h. vervielfältigt zur Verfügung stellen, darf er dies, soweit nicht Rechte und Freiheiten anderer Personen beeinträchtigt werden (vgl. Art. 15 Abs. 4 DS-GVO). Nur ein Anspruch darauf besteht nicht.

4.5 Geltendmachung eines Auskunftsersuchens gem. Art. 15 DS-GVO durch Bevollmächtigte

Macht jemand anderes als die betroffene Person deren Betroffenenrechte geltend, bedarf es einer Vertretungsbefugnis.

In der Praxis werden Auskunftsersuchen oftmals nicht nur durch die betroffenen Personen selbst, sondern durch Rechtsanwält:innen oder durch enge Familienangehörige, insbesondere Ehepartner:innen, gestellt.

Da es, wenn das Auskunftsrecht gem. Art. 15 DS-GVO nicht selbst durch die betroffene Person geltend gemacht wird, hierfür und für den Empfang der Auskunft einer Vertretungsbefugnis bedarf, sind Verantwortliche in einem solchen Fall gut beraten, sich das Vorliegen einer Vertretungsbefugnis sowohl für die Geltendmachung des Betroffenenrechts als auch den Empfang einer Auskunft nachweisen zu lassen.

Bei Rechtsanwält:innen gilt, dass, soweit die betroffenen Personen den Verantwortlichen nicht selbst von der anwaltlichen Vertretung in Kenntnis setzt, der Verantwortliche die Vorlage der

Originalvollmacht bei dem vertretenden Rechtsanwalt verlangen kann. Aus dieser ist ersichtlich, ob eine rechtsgeschäftliche Vertretung gegeben ist und inwieweit dies auch zur Geltendmachung des Auskunftsanspruchs und zum Erhalt der entsprechenden Auskunft bevollmächtigt.

Auch Ehepartner:innen sind nicht aufgrund etwaiger familienrechtlicher Regelungen (insbes. §§ 1357 ff. BGB) mit einer gesetzlichen Vertretungsbefugnis ausgestattet, um für den anderen Ehepartner eine Auskunft geltend zu machen und die Auskunft zu erhalten. Somit benötigt auch die/der Ehepartner:in, um für dessen Ehepartner:in eine Auskunft geltend zu machen, eine rechtsgeschäftliche Vertretungsvollmacht. Um eine Bevollmächtigung überprüfen zu können, kann der Verantwortliche ebenfalls die Vorlage einer Vertretungsvollmacht fordern, aus der hervorgeht, dass die/der vertretende Ehepartner:in dazu bevollmächtigt ist, ein Auskunftsersuchen für den/die betroffenen Ehepartner:in zu stellen und die Auskunft auch zu erhalten.

4.6 Geltendmachung des Auskunftsanspruchs durch Eltern

Zur Geltendmachung des Auskunftsanspruchs ist häufig ein Elternteil alleine befugt.

Im Rahmen verschiedener Beschwerdeverfahren war fraglich, ob ein Elternteil eine alleinige Vertretungsbefugnis bezüglich der Geltendmachung einen Auskunftsanspruch des minderjährigen Kindes hatte und in der Folge auch die Auskunft erhalten durfte.

Nach unserer Auffassung ist der Auskunftsanspruch zwar nicht abtretbar oder vererbbar, eine rechtliche Vertretung bei der Geltendmachung des eigenen Rechts ist jedoch grundsätzlich möglich.

Bei der Frage wer zur Vertretung bei der Geltendmachung des Auskunftsanspruches für das minderjährige Kind sowie den Empfang der Auskunft unter welchen Voraussetzungen befugt ist, muss je nach konkreter rechtlicher Situation differenziert werden:

Streitigkeiten entstanden in uns vorliegenden Fällen im Falle von getrenntlebenden bzw. geschiedenen Eltern, weshalb der vorliegende Beitrag sich auf dieses Szenario beschränkt.

Hier entscheidet letztlich die zivilrechtliche Rechtslage in welchen Konstellationen der Auskunftsanspruch durch ein Elternteil alleine geltend gemacht werden kann. Leben die Eltern getrennt und üben sie weiterhin das Sorgerecht gemeinsam aus, gilt für die Kompetenzverteilung nicht § 1627 BGB, vielmehr ist das sog. Residenzmodell als gesetzlicher Regelfall in § 1687 BGB normiert. Hiernach ist der Elternteil, bei dem das Kind seinen gewöhnlichen Aufenthalt hat, allein entscheidungsbefugt in Angelegenheiten des täglichen Lebens. Bei Angelegenheiten, die für das Kind von erheblicher Bedeutung sind, ist ein gegenseitiges Einvernehmen der Eltern erforderlich. Dies ist objektiv unter Berücksichtigung der individuellen Verhältnisse der jeweiligen Familie zu treffen. Verallgemeinert lässt sich jedoch sagen, dass Angelegenheiten dann von erheblicher Bedeutung sind, wenn sie nur schwer oder gar nicht abzuändernde Auswirkungen auf die Entwicklung des Kindes haben, bspw. Umgangsverbote, Aufenthaltsbestimmungen, Wechsel des Kindes in ein Heim, Entscheidungen über die Verwendung des Kindesvermögens betreffen (s. dazu Grüneberg, BGB, 81. Aufl. 2022, § 1687 Rn. 4 ff.). Angelegenheiten des täglichen Lebens sind dagegen der Schulalltag, die tägliche Pflege des Kindes (Nahrung, Kleidung, Hygiene), Routine-Erlaubnisse zur Freizeitgestaltung, gewöhnliche medizinische Versorgung bei leichteren Krankheiten (vgl. Grüneberg, ebd.).

Der Elternteil, bei dem das Kind nicht seinen gewöhnlichen Aufenthalt hat, hat dagegen (außer

im Falle einer Notvertretung) grundsätzliche keine Alleinvertretungsbefugnis, sondern nur ein Entscheidungsrecht in tatsächlicher Hinsicht, beschränkt auf Angelegenheiten der Betreuung.

Daraus ergibt sich nach unserer Interpretation Folgendes: Wenn beispielsweise ein Auskunftsanspruch über die personenbezogenen Daten des Kindes bei der behandelnden Kinderarztpraxis geltend gemacht werden soll, stellt dies, ebenso wie die Behandlung selbst, in der Regel (anders bspw. bei Entscheidung über Behandlung schwerer Erkrankungen) eine Angelegenheit des täglichen Lebens dar. Hierfür ist der Elternteil, bei dem das Kind seinen gewöhnlichen Aufenthalt hat, allein vertretungsbefugt, der andere Elternteil dagegen nicht.

Wenn die getrenntlebenden Eltern andere Betreuungsmodelle gewählt haben, bspw. das paritätische Wechselmodell, nach welchem die Betreuungsverantwortung zwischen den Eltern gleich verteilt ist und regelmäßig wechselt, erscheint es aus unserer Sicht vertretbar, dass jeder Elternteil das Auskunftsrecht alleine geltend macht.

Soweit nur ein Elternteil den Auskunftsanspruch gem. Art. 15 DS-GVO für sein minderjähriges Kind geltend macht, muss der Verantwortliche prüfen, inwieweit das Elternteil vertretungsberechtigt ist, damit nicht die Auskunft an das nicht vertretungsberechtigte Elternteil erteilt wird.

Wurde ein Auskunftsersuchen durch ein vertretungsberechtigtes Elternteil für das minderjährige Kind gestellt, so sollte die Auskunft zur Wahrung des Persönlichkeitsrechtes des Kindes an das minderjährige Kind selbst erteilt werden, soweit dieses einsichtsfähig ist.

5

Datenschutz im Internet

5 Datenschutz im Internet

5.1 Anforderungen an Cookie-Banner

Maßgebliche Anforderungen an Cookie-Banner werden zunehmend besser erfüllt. Künftig werden wir auch Apps dahingehend prüfen.

Auch wenn immer häufiger über neue Trackingtechnologien gesprochen wird, so betrifft die weit überwiegende Anzahl der Beschwerden und Kontrollanregungen im Bereich Internet noch immer den Einsatz von Cookies auf Webseiten. Wie wir unter Ziffer. 5.1 und 5.3 unseres letzten Tätigkeitsberichts ausgeführt haben, hat die DSK mit dem Inkrafttreten des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) im Dezember 2021 eine neue Orientierungshilfe für Anbieter:innen von Telemedien veröffentlicht. Diese hat 2022 ein Konsultationsverfahren durchlaufen, bei welchem wir maßgeblich mitgewirkt haben. Im Zuge dessen wurde auch ein 70-seitiger Auswertungsbericht erstellt, der auf die im Konsultationsverfahren aufgeworfenen Fragestellungen eingeht. In Anbetracht der begrenzten personellen Kapazitäten der Aufsichtsbehörden stellt dies ein nicht selbstverständliches Nebenprodukt dar. Dabei zeigt sich in der Praxis, dass sich der Aufwand gelohnt hat und ein durchaus positiver Trend hinsichtlich der Ausgestaltung von Cookie-Bannern auf Webseiten erkennbar ist.

Insbesondere das Erfordernis einer Ablehnoption auf erster Ebene ist bei den Webseitenbetreiber:innen angekommen, sodass vor allem die Anzahl der Anordnungen diesbezüglich nach Art. 58 Abs. 2 Buchst. d DS-GVO im Verlauf des Jahres 2022 nach einem anfangs starken Anstieg deutlich zurückgegangen ist.

Daneben müssen allerdings auch die weiteren Voraussetzungen, welche sich aus den Art. 4 Nr. 11, Art. 7 und ggfs. Art. 8 DS-GVO ergeben, eingehalten werden. Demnach muss eine Einwilligung vorab, freiwillig und informiert durch eine unmissverständliche Handlung erteilt werden. Hier zeigen sich bei der praktischen Umsetzung vor allem bei der Frage der Informiertheit noch Probleme. Gerade bei Webseiten, welche eine Vielzahl von Diensten einsetzen, ist es oftmals schwierig die Gradwanderung zwischen Informiertheit der Einwilligung und Informationsüberfluss zu bewältigen. Für Nutzer:innen stellt ein überladenes Banner ebenso wenig einen Mehrwert dar, wie ein Banner, das zu wenig Informationen enthält. Ein auch im Lichte der Datenminimierung ratsamer Ansatz kann daher sein, möglichst wenige Dienste einzusetzen.

In verschiedenen Prüfungen hat sich gezeigt, dass sich der insgesamt positive Trend noch nicht auf den Bereich „Apps“ ausgewirkt hat, sodass wir im kommenden Jahr verstärkt den Fokus auf die Prüfung von Apps legen wollen. Der rechtliche Rahmen für App-Tracking richtet sich - wie auch bei Webseiten - nach dem TTDSG und der DS-GVO. Es bedarf daher auch hier entsprechend § 25 Abs. 1 TTDSG im Regelfall einer Einwilligung, wenn auf die Endeinrichtung – hier: das Smartphone – zugegriffen wird. In der Realität erfolgen meist aber schon zahlreiche Zugriffe bereits bei erstem Öffnen der App, noch bevor überhaupt eine Auswahl über ein Consent-Banner getroffen werden kann.

5.2 Abo-Modelle

Bezahlvariante als Alternative zur Einwilligung grundsätzlich zulässig.

Spätestens durch die Orientierungshilfe für Anbieter:innen von Telemedien 2021 haben die deutschen Aufsichtsbehörden zum Ausdruck gebracht, dass die Anforderungen an eine rechtswirksame Einwilligung auch im Webseitenkontext vollständig erfüllt sein müssen. Wir haben hierzu im letzten Tätigkeitsbericht unter

Ziff. 5.3 bereits berichtet. Diese Anforderungen nehmen nun immer mehr Verantwortliche zum Anlass auf ein sog. Abo- Modell, wie es bereits von einigen Medienhäusern betrieben wird, umzustellen. Bei der klassischen Variante bedeutet dies, dass eine Einwilligung über ein Consent-Banner eingeholt werden soll und die Möglichkeit abzulehnen darin besteht, ein kostenpflichtiges Abonnement abzuschließen. Auf diesem Wege kann grundsätzlich eine rechtswirksame Einwilligung entsprechend Art. 6 Abs. 1 Buchst. a DS-GVO eingeholt werden. Insbesondere ist das Merkmal der „Freiwilligkeit", welches sich aus Art. 4 Nr. 11 DS-GVO und Erwägungsgrund 43 ergibt nicht bereits dadurch ausgeschlossen, dass die angebotene Alternative kostenpflichtig ist. Sofern die Bezahlvariante ein marktübliches Entgelt fordert, kann diese eine gleichwertige Alternative darstellen. Im Regelfall bietet sich diese Gestaltung daher auch nur an, wenn durch die Website Inhalte bereitgestellt werden, für die üblicherweise ein Entgelt in Betracht kommt. Den Zugang bspw. zu einem Onlineshop hinter eine solche Abo-Schranke zu setzen wäre daher genauer zu prüfen. Allerdings wird dies wohl kaum im Sinne der Betreiber:innen sein, da hier der Verkauf von Produkten das eigentliche Ziel ist und nicht nur der Besuch der Website.

Daneben müssen allerdings auch die weiteren Voraussetzungen für eine rechtswirksame Einwilligung entsprechend Art. 4 Nr.11, Art. 7 DS-GVO und ggfs. Art. 8 DS-GVO eingehalten werden. Dies bedeutet unter anderem auch, dass eine Einwilligung granular möglich sein muss und nicht nur ein pauschales „Alle Akzeptieren" angeboten werden darf. Instruktiv ist insoweit auch der zwischenzeitlich ergangene DSK Beschluss zur Bewertung von Pur-Abo-Modellen auf Websites.

5.3 „Bezahlen mit Daten".

Die BGB-Novelle schafft keine neue datenschutzrechtliche Rechtsgrundlage.

Anfang 2022 wurden die Verbraucherschutzvorschriften des BGB im Rahmen der Umsetzung der Digitale-Inhalte-Richtlinie novelliert. Aus datenschutzrechtlicher Sicht ist hier vor allem relevant, dass in § 312 Abs. 1a BGB, sowie in den §§ 327 ff. BGB das Bereitstellen von personenbezogenen Daten einem Bezahlen mit Geld gleichgestellt wird. Hierzu hat die Datenschutzkonferenz am 29.11.2022 den Beschluss „Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht" veröffentlicht. In dem Beschluss wird im Kern dargestellt, dass die neuen Verbraucherschutzvorschriften, welche das umgangssprachlich als „Bezahlen mit Daten" bezeichnete Konzept in den Anwendungsbereich aufnehmen, keine eigene datenschutzrechtliche Rechtsgrundlage darstellen. Dies bedeutet, dass unabhängig davon, ob der Anwendungsbereich der Verbraucherschutzvorschriften des BGB eröffnet ist, eine Rechtsgrundlage nach Art. 6 DS-GVO erforderlich ist. Eine Datenverarbeitung kann in diesem Zusammenhang nicht auf die BGB- Normen gestützt werden. Im Webseitenkontext kommt hier vor allem die Einwilligung, die Vertragsgrundlage oder auch ein berechtigtes Interesse in Betracht.

In der Praxis wurden uns in aufsichtlichen Verfahren oder auch im Rahmen unserer Beratungstätigkeiten verschiedene Modelle vorgestellt, die teilweise noch nicht abschließend geprüft worden sind. Neben der unter Ziffer 5.2 („Abo-Modelle") dargestellten „klassischen" Einwilligungsvariante, ist auch vermehrt die „Vertragslösung" vorgestellt worden. Hierbei soll gerade keine Einwilligung nach Art. 6 Abs. 1 Buchst. a DS-GVO eingeholt werden, sondern ein Vertrag über die Nutzung der Website abgeschlossen werden. Im Regelfall haben Nutzer:innen dann die Wahl, das bereitgestellte An-

gebot gegen Bezahlung eines Entgelts wahrzunehmen oder sie verpflichten sich, dem Verantwortlichen personenbezogene Daten bereitzustellen. Dies widerspricht auch nicht den jüngst ergangenen Entscheidungen des EDSA (Binding Decision 3/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Facebook service (Art. 65 GDPR)) und den Ausführungen in den Leitlinien 2/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DS-GVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen. Denn bei dieser Konstellationen verpflichten sich Nutzer:innen zur Bereitstellung ihrer Daten; dies stellt damit eine Hauptleistungspflicht der Nutzer:innen dar. Eine Verarbeitungspflicht für den Verantwortlichen ergibt sich dadurch nicht. Damit dieses Modell datenschutzkonform abgebildet werden kann, ist es erforderlich, dass zunächst überhaupt ein wirksamer Vertrag vorliegt. Ob und wann zwischen Nutzer:innen und Betreiber:innen einer Webseite, deren Angebote durch personalisierte Werbung (teilweise) finanziert werden, tatsächlich ein Vertrag über digitale Produkte zustande kommt, richtet sich nach den allgemeinen Grundsätzen des Zivilrechts.

Die Frage ob ein wirksamer zivilrechtlicher Vertragsschluss vorliegt, kann von den Datenschutzaufsichtsbehörden als zivilrechtliche Vorfrage letztlich, wie in allen Verarbeitungstätigkeiten, die sich auf die Rechtsgrundlage Art. 6 Abs. 1 Buchst. b DS-GVO stützen, nicht abschließend überprüft werden. Grundsätzlich nachzuweisende Mindestanforderungen sind jedenfalls die essentialia negotii, also Gesamtumstände aus denen erkennbar wird, wer Vertragspartner ist, außerdem die Leistung, sowie die verlangte Gegenleistung bzw. - im Falle eines Bereitstellens von Daten anstelle eines Entgelts - welche Daten bereitgestellt werden müssen, über welchem Zeitraum, welche Dritten hierauf Zugriff erhalten und wie der vertragliche Leistungsaustausch beendet werden kann.

Damit das Bereitstellen von Daten wirksam als Primärzweck vertraglich vereinbart und damit zur Vertragserfüllung als erforderlich angesehen werden kann, sind die generellen Voraussetzungen des Art. 6 Abs. 1 Buchst. b DS-GVO zu erfüllen. Dies gilt insbesondere im Hinblick auf die Zweckbeschreibung. Diese muss spezifisch, transparent und granular erfolgen, um abzugrenzen was zur Vertragserfüllung erforderlich ist. Darüber hinausgehende Zwecke bedürfen einer eigenen Rechtsgrundlage. Für Nutzer:innen muss erkennbar sein, wozu sie sich ganz konkret verpflichten, bzw. was zur Vertragserfüllung erforderlich ist. Um dies sicherzustellen muss eine gewisse, für Nutzer:innen nachvollziehbare Begrenzung vorgenommen werden, da ein pauschales Bereitstellen von personenbezogenen Daten für eine Vielzahl von Diensten – ebenso wie bei einer Einwilligung - nicht vereinbart werden kann. In der Praxis könnte es sich daher anbieten, Nutzer:innen eine Auswahlmöglichkeit anzubieten, bspw. indem vorgegeben wird, in welchem Umfang bzw. welche Zahl von Empfängern personenbezogene Daten bereitgestellt werden, um digitale Inhalte abrufen zu können. Daneben sind in diesem Kontext auch bei dieser Konstellation die Vorgaben aus Art. 9 und Art. 21 DS-GVO zu beachten.

5.4 Apple „Look-Around"

Die Veröffentlichung von Bildern, wie beispielsweise dem eigenen Haus, kann im Rahmen des Apple „Look- Around"- Features, kann im Regelfall auf ein berechtigtes Interesse nach Art. 6 Abs. 1 Buchst. f DS-GVO gestützt werden.

Im April 2021 wurde mit der Einführung des sog. Look-Around-Features von Apple begonnen. Mittels diesem werden 3D-Ansichten des Kartenmaterials dargestellt, wodurch es zu Veröffentlichungen von personenbezogenen Daten wie Häuserfronten oder auch Bildern von Personen kommt. Apple hat die schrittweise Einführung dieses Features mit dem BayLDA abge-

stimmt und hierzu auch den Umgang mit Widersprüchen und die technische Umsetzung erläutert.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat bereits am 12.05.2020 einen Beschluss zu Vorabwidersprüchen bei StreetView und vergleichbaren Diensten veröffentlicht, der sich zur Zulässigkeit der vorgelagerten Kamerafahrten und den möglichen nachfolgenden Veröffentlichungen äußert. Über dieses Thema haben wir im Hinblick auf die Apple Kamerafahrten im Tätigkeitsbericht 2020 unter Punkt 5.4 berichtet.

Der Beschluss stellt fest, dass auch bei der Veröffentlichung von Straßenansichten, einschließlich teilweiser Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, welche an den öffentlichen Straßenraum angrenzen, im Rahmen von StreetView und ähnlichen Diensten Art. 6 Abs. 1 Buchst. f DS-GVO als Rechtsgrundlage in Betracht kommen kann. Sofern die dort genannten Voraussetzungen erfüllt sind, ist nicht ersichtlich, weshalb eine andere Bewertung als bei dem Dienst „Google Streetview" vorgenommen werden sollte. Apple bietet – wie von der Datenschutzkonferenz gefordert – die Möglichkeit an, personenbezogene Daten (etwa Gesichter, Fahrzeugkennzeichen, Häuserfassaden) unkenntlich machen zu lassen; betroffene Personen können dies durch Einlegung eines Widerspruchs beantragen.

Dieses Verlangen kann zumindest ab dem Zeitpunkt der Anfertigung der Aufnahmen durch den Dienst wahrgenommen werden. Art. 21 DS-GVO bleibt unberührt. Das Verlangen auf Unkenntlichmachung nach Art. 17 Abs. 1 DS-GVO und der Widerspruch nach Art. 21 DS-GVO müssen sowohl online als auch postalisch eingelegt werden können. Auf diese Rechte muss ausdrücklich hingewiesen werden.

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

Apple Distribution International
Data Protection Officer
Hollyhill Industrial Estate
Cork
Irland

Weiterhin ist dies auch elektronisch per eMail (MapsImageCollection@apple.com) oder über das Kontaktformular unter: https://www.apple.com/privacy/contact/ möglich.

Widersprüche, die bereits im Rahmen der Apple Kamerafahrten bzw. als Vorabwidersprüche eingelegt worden sind, bleiben bestehen.

Aufgrund der Tatsache, dass der europäische Hauptsitz des Unternehmens in Irland ist, handelt es sich hierbei im Regelfall um grenzüberschreitende Verarbeitungen. Dies bedeutet, dass Beschwerden die bei uns eingehen, nicht alleine durch unsere Behörde bearbeitet werden, sondern entsprechend den Vorgaben der DS-GVO im Rahmen des Kooperations- und Kohärenzverfahrens. Die Federführung obliegt dabei der irischen Aufsichtsbehörde.

6

Rechtsanwält:innn und andere freie Berufe

6 (Hoch)Schulen und Bildungseinrichtungen

6.1 Videoaufzeichnungen im Hochschulkontext

Videoaufzeichnungen an Hochschulen sind, wenn überhaupt, nur mit Einwilligung der betroffenen Personen zulässig.

Eine private Hochschule bat uns im Berichtszeitraum um Einschätzung zu der Frage, ob und ggf. unter welchen Voraussetzungen Lehrveranstaltungen sowie Online-Prüfungen per Video aufgezeichnet werden dürfen.

Wir wiesen darauf hin, dass die Videoaufzeichnung von Lehrveranstaltungen nur mit wirksamer Einwilligung der betroffenen Personen zulässig ist. Denn im bayerischen Hochschulrecht gibt es keine gesetzlichen Vorschriften, auf die sich eine entsprechende Verarbeitungsbefugnis stützen ließe. Von der Fragestellerin wurde zwar erläutert, dass Hochschulen die Aufgabe haben, Inhalte und Formen des Studiums im Hinblick auf u.a. die notwendigen Veränderungen in der Berufswelt weiterzuentwickeln. Diese Aufgabenzuweisung erfüllt jedoch nicht die Maßgaben des Art. 6 Abs. 3 DS-GVO, insb. fehlt es an einer Festlegung der konkreten Verarbeitungszwecke. Videoaufzeichnungen lassen sich nach unserer Auffassung auch nicht über berechtigte Interessen der Hochschulen begründen, da insoweit die entgegenstehenden Interessen der betroffenen Personen überwiegen.

Was die Aufzeichnung von Online-Prüfungen angeht, so hat der bayerische Gesetzgeber von der Verordnungsermächtigung gem. Art. 61 Abs. 10 BayHSchG a.F. Gebrauch gemacht und spezifische Regelungen in der Bayerischen Fernprüfungserprobungsverordnung (BayFEV) erlassen. § 6 Abs. 3 S. 1 BayFEV bestimmt ausdrücklich, dass eine Aufzeichnung der Prüfungen oder eine anderweitige Speicherung der Bild- und Tondaten unzulässig sind. Dies gilt auch für mündliche und praktische Fernprüfungen (§ 7 Abs. 2 S. 1 BayFEV). In diesem Bereich ist also auch mit Einwilligung der betroffenen Personen keine Aufzeichnung möglich, insb. dürfte eine solche Einwilligung aufgrund der bestehenden Drucksituation auch nicht freiwillig sein.

7

Versicherungswirtschaft und Banken

7 Versicherungswirtschaft

7.1 Bearbeitung medizinischer Unterlagen innerhalb einer Versicherung

Versicherungsnehmer:innen haben keinen Anspruch darauf, dass ihre im Rahmen der Leistungsprüfung eingereichten medizinischen Unterlagen in sämtlichen Versicherungssparten ausschließlich von Gesellschaftsärzt:innen bearbeitet werden.

In einer Beschwerde gegen ihre Berufsunfähigkeitsversicherung beanstandete die Beschwerdeführerin, dass von ihr im Rahmen der Leistungsprüfung vorgelegte Unterlagen (darunter u.a. ein Bericht einer psychiatrischen Fachärztin) nicht ausschließlich von medizinischem Fachpersonal bearbeitet worden seien. Die Beschwerdeführerin berief sich in diesem Zusammenhang auf eine Abstimmung zwischen den Datenschutzaufsichtsbehörden und der Versicherungswirtschaft betreffend private Krankenversicherungen. Letztere sollen vergleichbare Berichte direkt von ihren Gesellschaftsärzt:innen sichten lassen, die den Sachbearbeiter:innen lediglich das Ergebnis der Prüfung, nicht aber die zugrundeliegenden Unterlagen übermitteln.

Anlässlich dieser Beschwerde tauschten wir uns mit den anderen deutschen Datenschutzaufsichtsbehörden sowie der Versicherungswirtschaft darüber aus, ob die für die private Krankenversicherung abgestimmten Vorgaben ohne weiteres auf andere Versicherungssparten übertragen werden können. Dies wurde im Ergebnis verneint, insb. da in anderen Versicherungssparten nicht ausschließlich medizinische Fragen zu beantworten sind.

Unabhängig hiervon gelten für alle Versicherungsunternehmen die Vorgaben des Art. 32 DS-GVO, insb. die Pflicht zur Vorhaltung risikoadäquater technischer und organisatorischer Maßnahmen.

8

Finanzwirtschaft

8 Finanzwirtschaft

8.1 Erzwungene Datenschutzeinwillligung bei Kontovertrag

Eine durch Zwang und/oder entsprechende Vorankreuzungen des Verantwortlichen erteilte Einwilligung ist nicht freiwillig und damit unwirksam.

Uns erreichte die Beschwerde eines kürzlich volljährig gewordenen Betroffenen, welcher bei einer bayerischen Bank aus diesem Anlass einen neuen eigenen Vertrag zur Fortführung der bestehenden Geschäftsbeziehung abschließen wollte.

Hierzu erhielt er von der Bank einen Vertragsvordruck zur Unterschrift, in welchem die Felder zur freiwilligen Erteilung von datenschutzrechtlichen Einwilligungen, die zur eigentlichen Vertragsdurchführung nicht erforderlich sind (hier beispielsweise Verarbeitungen zum Zweck einer individuellen werblichen Ansprache über verschiedene Kommunikationskanäle) derart vorangekreuzt waren, dass die Einwilligungen mit der Unterschrift als erteilt gelten sollten.

Auf die Bitte des Betroffenen hin, dass er eine Vertragsversion ohne Erteilung dieser Einwilligungen wünsche, wurde ihm von der Bank mitgeteilt, dass ohne Erteilung der Einwilligungen eine Kündigung der bestehenden Geschäftsbeziehung erfolgen würde.

Die Bank hat von uns eine aufsichtliche Warnung erhalten, da es unzulässig ist, die Erteilung einer grundsätzlich freiwilligen datenschutzrechtlichen Einwilligung an die Frage des Fortbestands oder des Abschlusses eines Vertrags zu koppeln. Darüber hinaus betrachten wir bereits das Vorankreuzen der Auswahlfelder einer Einwilligungserklärung als unzulässig.

Wir verwiesen in diesem Zusammenhang auf Art. 7 DS-GVO i.V.m. der Guideline 05/2020 des Europäischen Datenschutzausschusses zur Einwilligung gemäß Verordnung 2016/679.

Insbesondere aus Gründen der erforderlichen Freiwilligkeit einer Einwilligung sind Einwilligungen, die auf diese Art und Weise zustande kommen, unwirksam, sodass auch hierauf aufbauende Verarbeitungen datenschutzrechtlich unzulässig sind.

8.2 Cent-Überweisung im Vorfeld einer Kontopfändung

Nutzt ein Inkassobüro Banküberweisungen als Kommunikationsmittel, ist dies in aller Regel unzulässig. Es gibt jedoch auch besondere Anwendungsfälle, die datenschutzrechtlich zulässig sein können.

Wir erhielten die Beschwerde einer Betroffenen, da ein Inkassobüro ihr eine niedrige Summe im Cent-Bereich auf ihr Bankkonto überwiesen hatte. In der Überweisung war als Verwendungszweck eine Rückrufbitte zu einem sie betreffenden Inkassovorgang enthalten.

Eine Nutzung von Überweisungen als Kommunikationsmittel durch ein Inkassobüro ist in den meisten Anwendungsfällen unzulässig. Diese Praxis erzeugt mehrere Probleme von einer Offenlegung des Inkassovorgangs gegenüber der Bank bis hin zur praktischen Irreversibilität der Überweisung im Falle eines Fehlers.

Im Zuge unserer Prüfung des Sachverhalts beim verantwortlichen Inkassobüro zeigte sich jedoch, dass dieses solche Überweisungen tatsächlich nicht zum Zweck einer Kontaktaufnahme im Stadium eines womöglich noch fraglichen Forderungsbestands vornimmt, sondern ausschließlich, um unmittelbar vor einer Kon-

topfändung zu prüfen, ob die bekannte Bankverbindung noch existiert. In den Anwendungsfällen ist somit zudem immer bereits ein Forderungstitel vorhanden; der Bestand der Forderung steht also nicht mehr in Frage. Der hierbei überwiesene Cent-Betrag wird den Schuldner:innen nicht in Rechnung gestellt.
Die im Verwendungszweck enthaltene Bitte um Rückruf war insofern eher als missglückte Formulierung zu betrachten, die zunächst eine Verwendung als bloßes Kommunikationsmittel nahelegte.

Zu dem Zweck und Zeitpunkt, zu welchem das Inkassobüro dieses Mittel verwendet, gehen wir insgesamt von einem für die Zulässigkeit ausreichenden berechtigten Interesse des Inkassobüros aus, zumal diese Methode beispielsweise auch dazu dienen kann, die im Falle eines nicht mehr existenten Kontos beim Pfändungsversuch erfolglos anfallenden Datenübermittlungen und Zusatzkosten zu vermeiden. Die vom Inkassobüro aufgezeigte Quote von Kontopfändungen, die ohne dieses Mittel ins Leere laufen würden, war ausreichend hoch um eine entsprechende Erforderlichkeit zu begründen.

Wir haben im Fall des hier betrachteten Inkassobüros deshalb letztlich lediglich veranlasst, dass der Verwendungszweck solcher „Testüberweisungen" datensparsamer ausgestaltet wird. Zukünftig wird dieser lediglich noch die Aktennummer des Inkassobüros enthalten.

8.3 Kontaktaufnahme durch Anlagevermittler:innen bei Insolvenz der vermittelten Anlage

Informationen zum Insolvenzverfahren durch Vermittler:innen der insolventen Anlage sind zwar möglich, müssen aber so neutral und objektiv wie möglich ausgestaltet sein.

Im zu prüfenden Fall ist ein Unternehmen, bei welchem die betroffenen Personen Anlagen in Form von Nachrangdarlehen gezeichnet hatten, in Insolvenz geraten. Die von der Insolvenz selbst nicht unmittelbar betroffene Vermittlerin der Anlage kontaktierte daraufhin die von der Insolvenz betroffenen Anleger:innen, um diesen Informationen zum Insolvenzverfahren bereitzustellen und diese auf die Möglichkeit der Bevollmächtigung von Stimmrechtsvertreter:innen für den Gläubigerausschuss hinzuweisen, wobei auch eine Auswahl von mehreren bereits durch andere Personen bevollmächtigten Vertreter:innen (insbesondere Anwält:innen) und ein entsprechendes Formblatt zur Erteilung einer Stimmrechtsvollmacht mitgesandt wurde.

Wir erhielten diesbezüglich Beschwerden, die von einer unzulässigen Verarbeitung und Werbemaßnahme der Vermittlerin zugunsten der genannten Anwält:innen ausgingen, um im Gläubigerausschuss eine der Insolvenzschuldnerin gewogene Mehrheit zu erreichen.

Bei unserer Prüfung kamen wir zu dem Ergebnis, dass zum einen die im konkreten Schreiben enthaltenen Informationen die Grenze zu einer Werbemaßnahme noch nicht überschritten haben und zum anderen die Verarbeitung durch die Vermittlerin der notleidenden Verträge beim vorliegenden Inhalt noch als zur Vertragserfüllung erforderliche Verarbeitung gerechtfertigt werden kann.
Allerdings machten wir der Vermittlerin auch deutlich, dass die Ausgestaltung ihrer Schreiben an die betroffenen Personen die Grenzen einer solchen nachvertraglichen Information erreicht, indem darin zumindest Tendenzen zur Werbung und zu Handlungsappellen enthalten waren.
Die genutzte datenschutzrechtliche Zulässigkeitsnorm verlangt aus unserer Sicht, dass derartige Schreiben so neutral und objektiv wie möglich ausgestaltet werden und eindeutig von einem werblichen Charakter oder konkreten Handlungsappellen abgrenzbar sind.

8.4 Verarbeitung der Steuer-ID und Nutzung einer abweichenden Anschrift bei Betreuer:innen

Die Erhebung der Steuer-ID von Betreuer:innen kann unzulässig sein. Geben Betreuer:innen bei der Bank eine abweichende Versandanschrift an, ist diese in aller Regel auch zu berücksichtigen.

Wir haben in mehreren Fällen gegen verschiedene bayerische Banken Beschwerden dahingehend erhalten, dass diese auch von Betreuer:innen im Sinne der §§ 1896 ff. BGB, die selbst nicht gleichzeitig eine eigene Geschäftsverbindung bei der Bank unterhalten, unter Bezugnahme auf die Abgabenordnung (AO) deren Steuer-ID erheben möchten.

Gemäß § 139b Abs. 2 Satz 2 Nr. 1 AO dürfen Kreditinstitute die Steuer-ID betroffener Personen nur dann ohne deren Einwilligung verarbeiten, wenn eine Rechtsvorschrift dies ausdrücklich erlaubt oder anordnet, oder die Verarbeitung zwischen dem Kreditinstitut und den Finanzbehörden erforderlich ist.

Zwar ordnet § 154 Abs. 2a Satz 1 AO grundsätzlich die Erhebung und Aufzeichnung der Steuer-ID von Verfügungsberechtigten an. Der Gesetzgeber hat diesbezüglich jedoch in § 154 Abs. 2d AO die Möglichkeit von Erleichterungen vorgesehen.
Von dieser Möglichkeit von Erleichterungen wurde in Bezug auf die rechtliche Betreuung nach §§ 1896 ff. BGB im AO-Anwendungserlass (AEAO) zu § 154 unter Nr. 11.1 lit. b Gebrauch gemacht, sodass es bei solchen Betreuer:innen an einer Anordnung durch Rechtsvorschrift sowie an einer Erforderlichkeit im Sinne des § 139b Abs. 2 Satz 2 Nr. 1 AO fehlt.

Dies führt insgesamt regelmäßig dazu, dass bezüglich der durch den AEAO vorgesehenen Erleichterungen das Ergebnis der datenschutzrechtlichen Erforderlichkeitsprüfung ein Verzicht auf die Erhebung sein muss. Abweichungen hiervon müssten entsprechend begründet und im Sinne des Art. 5 Abs. 2 DS-GVO dokumentiert werden.
In dem Fall, dass Betreuer:innen außerhalb ihrer Betreuungsrolle parallel auch eine eigene Geschäftsbeziehung zur Bank unterhalten, greift die genannte Erleichterung natürlich nicht auch für die eigene Geschäftsbeziehung.

Weiter wurde uns von Betreuer:innen, die bei einem Betreuungsverein tätig sind, jeweils vorgetragen, dass die Bank die Angabe des Betreuungsvereins als abweichende Anschrift regelmäßig ignoriere und somit Unterlagen mit Daten der betreuten Person an die Privatanschrift der Betreuer:innen versende. Dort bestehe dann die Gefahr, dass die Daten zur Kenntnis von Familienmitgliedern gelangen.

Hier kamen wir zu dem Ergebnis, dass die Bank, auch wenn ihr gleichzeitig die Privatanschrift von Betreuer:innen bekannt ist, eine von diesen für das Betreuungsverhältnis angegebene abweichende Anschrift im Rahmen der Datensicherheit zu berücksichtigen hat. Nach unseren Kenntnissen stehen in der Branche der Kreditwirtschaft durchgängig auch die technischen Voraussetzungen zur Verfügung, um hier eine hinreichende Trennung zu gewährleisten.

Es kann hier allerdings auch Einzelkonstellationen geben, in denen besondere Bedingungen eine ausnahmsweise Abweichung von diesem Grundsatz getrennter Versandverwaltung rechtfertigen. Wenn Betreuer:innen beispielsweise selbst für das Betreuungsverhältnis einen Teilnahmevertrag am Online-Banking abschließen, so ist es gerechtfertigt, dass der Versand der Zugangsdaten direkt an die Betreuer:innen erfolgt, statt an den angegebenen Betreuungsverein.
Regelmäßiger Grundsatz bleibt jedoch, dass bei angegebener abweichender Anschrift für ein Betreuungsverhältnis diese auch zu berücksichtigen ist.

9

Handel und Dienstleistung

9 Handel und Dienstleistung

9.1 Novellierung der Heizkostenverordnung

Funkmessgeräte zur Messung des Heiz- und Warmwasserverbrauchs sind verpflichtend, es gibt kein Widerspruchsrecht gegen die Datenverarbeitung in diesem Zusammenhang.

Insbesondere im ersten Quartal des Berichtszeitraums erreichten uns zahlreiche Anfragen, vereinzelt auch Beschwerden, hinsichtlich der Novellierung der Heizkostenverordnung (HeizkostenV) die im November 2021 in Kraft getreten ist, mit der die funkbasierte verbrauchsabhängige Erfassung und Abrechnung von Heiz- und Warmwasserkosten, somit also insbesondere der Einbau von Funkzählern von den Vermieter:innen gefordert wird.

Dabei beschränkten sich die Anfragen jedoch nicht auf die Funkzähler, die zur Messung von Wärme und Warmwasser eingebaut wurden, sondern oftmals wurden weitere Verbrauchsmessungen und auch „datenschutzfremde" Fragestellungen in den Anfragen vermischt. Dies hatte teilweise zur Folge, dass den Eingabeführern zunächst einmal die Rechtslage und der Anwendungsbereich des Datenschutzrechts dargestellt werden mussten, bevor konkrete Informationen betreffend die HeizkostenV und der darin enthaltenen Regelungen gegeben werden konnten.

Um den Heiz- und Warmwasserverbrauch der Nutzer:innen (also der Mieter:innen oder selbstnutzende WEG-Eigentümer:innen) messen zu können, müssen nunmehr Funkzähler eingebaut werden, die den in der HeizkostenV festgelegten Kriterien (vgl. § 5 HeizkostenV) entsprechen. Entsprechen die Funkzähler den festgelegten Kriterien, kann sich die/der Nutzer:in auch nicht gegen den Einbau eines bestimmten Modells wehren bzw. den Einbau eines konkreten Modells verlangen. Ein Widerspruchsrecht gegen den Einbau eines Funkzählers zur Messung des Heiz- und Wärmeverbrauchs besteht nicht. Auch wenn in § 4 Abs. 2 HeizkostenV ein Widerspruchsrecht der Nutzer:innen geregelt wird, so betrifft dieses allein die Frage der Kostentragung durch die Nutzer:innen, wenn der/die Gebäudeeigentümer:in die Ausstattung mieten möchte. Der Einbau und die Datenverarbeitung können hierdurch jedoch nicht verhindert werden.

Den anfragenden Personen war häufig nicht klar, dass die Verantwortlichkeit für die Datenverarbeitung im Zusammenhang mit der funkbasierten Heiz- und Warmwasserverbrauchsmessung bei den Gebäudeeigentümer:innen bzw. diesen gleichgestellten Personen (vgl. § 1 Abs. 2 HeizkostenV) liegt. Dies gilt auch dann wenn ein Ableseunternehmen eingebunden ist, welches ggf. zugleich die Funkzähler eingebaut hat. I.d.R. agieren die Ableseunternehmen im Rahmen einer Beauftragung durch den/die Gebäudeeigentümer:in, d.h. als Auftragsverarbeiter gem. Art. 4 Nr. 8 DS-GVO.

10 Internationaler Datenverkehr

10.1 Was ist eine Übermittlung in ein Drittland?

Der Europäische Datenschutzausschuss hat erstmals Hinweise dazu vorgelegt, in welchen Fällen nach Auffassung der Aufsichtsbehörden von einer „Übermittlung personenbezogener Daten in ein Drittland" ausgegangen werden sollte.

Zahlreiche Verarbeitungen personenbezogener Daten haben einen Bezug zu so genannten

Drittländern, d.h. Ländern, die keine Mitgliedstaaten der Europäischen Union sind und auch nicht dem Europäischen Wirtschaftsraum angehören. Beispielhaft genannt seien die USA, aus denen die Anbieter zahlreicher Cloud-Dienste stammen, die in weitem Umfang auch von Unternehmen und anderen Akteuren in der Europäischen Union täglich eingesetzt werden. Für Fälle der Übermittlung personenbezogener Daten in Drittländer müssen Verantwortliche und Auftragsverarbeiter gemäß Artikel 44 DS-GVO die Anforderungen des fünften Kapitels der DS-GVO einhalten und somit für eine solche Übermittlung etwa so genannte Standdarddatenschutzklauseln nach Art. 46 Abs. 2 Buchst. c DS-GVO verwenden. Nicht jede Verarbeitung personenbezogener Daten mit Drittlandsbezug stellt jedoch im Gesetzessinne eine Übermittlung personenbezogener Daten in ein Drittland dar. Bedauerlicherweise enthält die DS-GVO selbst jedoch keine Definition des Begriffs „Übermittlung in ein Drittland", so dass bei Unternehmen und anderen Akteuren häufig Unsicherheit besteht, wann eigentlich von einem solchen Fall auszugehen ist. Nach umfangreichend Beratungen hat der Europäische Datenschutzausschuss (EDSA) bereits Ende 2021 versucht, im Wege eines Leitlinienpapiers die Interpretation dieses Begriffs aus Sicht der Aufsichtsbehörden zu erläutern und damit den Rechtsanwendern praktische Hilfe in dieser Frage an die Hand zu geben. Nach einer öffentlichen Konsultation hat der Europäische Datenschutzausschuss inzwischen die Nach-Konsultations-Fassung des Papiers veröffentlicht, auf das an dieser Stelle aufgrund der großen Bedeutung des Papiers verwiesen werden soll, auch wenn das Datum der Verabschiedung mit dem 24.02.2023 schon nach Ende des vorliegenden Berichtszeitraums liegt.

Nach der Interpretation des EDSA liegt eine Übermittlung personenbezogener Daten in ein Drittland demnach dann vor, wenn

- ein Verantwortlicher oder Auftragsverarbeiter, der mit der in Rede stehenden Verarbeitung unter die DS-GVO fällt („Datenexporteur"),
- personenbezogene Daten an einen anderen Verantwortlichen, gemeinsam Verantwortlichen oder Auftragsverarbeiter offenlegt oder bereitstellt,
- und zwar dergestalt, dass sich der empfangende Verantwortliche, gemeinsam Verantwortliche oder Auftragsverarbeiter in einem Drittland befindet („Datenimporteur"), und zwar auch dann, wenn er für die betreffende Verarbeitung selbst unter den Anwendungsbereich der DS-GVO nach Art. 3 DS-GVO fällt.

Damit werden eine Reihe der typischerweise klärungsbedürftigen Fragen in diesem Zusammenhang jedenfalls in der Positionierung des EDSA geklärt. So ist etwa ein Fernzugriff eines/einer auf Geschäftsreise in einem Drittland befindlichen Beschäftigten auf eine bei seinem Arbeitgeber in der EU befindliche Datenbank mit personenbezogenen Daten keine „Übermittlung in ein Drittland", weil der/die Zugriff nehmende Beschäftigte kein (von seinem Arbeitgeber) separater Verantwortlicher oder Auftragsverarbeiter ist. Ebenso liegt eine „Übermittlung in ein Drittland" nicht vor, wenn die betroffene Person ihre Daten selbst dem in einem Drittland befindlichen Verantwortlichen bereitstellt, etwa durch Direkteingabe in ein Online-Formular; denn in einem solchen „Direkterhebungsfall" ist nur ein einziger Verantwortlicher an dem Datenfluss beteiligt, es gibt also keinen vom Datenimporteur zu unterscheidenden Datenexporteur.

Zu der Frage, wann eigentlich bei Vorhandensein eines übermittelnden Verantwortlichen bzw. Auftragsverarbeiters und eines davon separaten empfangenden Verantwortlichen bzw. Auftragsverarbeiters der Empfänger „in einem Drittland ist" und somit eine Datenübermittlung in ein Drittland vorliegt, wendet der EDSA einen gemischten Ansatz an, der sowohl geographische als auch jurisdiktionale Elemente enthält. Eine Drittlandsübermittlung ist demnach zu bejahen, wenn etwa ein US-Unternehmen (etwa

eine als „Inc." in den USA eingetragene Gesellschaft) personenbezogene Daten zur Verarbeitung (auch) außerhalb des EU-Territoriums erhält. Handelt es sich hingegen beim Empfänger um ein „EU-/EWR-Unternehmen" und verarbeitet dieser die Daten geographisch (einschließlich etwaiger Fernzugriffe) ausschließlich innerhalb des EWR, liegt nach der Interpretation des EDSA keine Übermittlung in ein Drittland vor. Dies gilt ausweislich des Beispiels 12 im EDSA-Papier sogar dann, wenn das EWR-Unternehmen eine in einem Drittland ansässige Muttergesellschaft hat und aufgrund dieses Umstands unter extraterritorial anwendbare Rechtsvorschriften des Drittlands fällt, die für Behörden dieses Drittlands grundsätzlich die Möglichkeit enthalten, das EWR-Unternehmen (und/oder dessen Muttergesellschaft) zur Herausgabe von im EWR (durch das EWR-Unternehmen) verarbeitete personenbezogene Daten aufzufordern. Solange in einem solchen Fall das EWR-Unternehmen die Daten aus Anlass einer solchen Aufforderung (noch) nicht an die Drittlandsbehörde übermittelt hat, liegt nach EDSA-Ansicht noch keine Übermittlung in ein Drittland vor, so dass Kapitel V DS-GVO nicht zur Anwendung kommt. Allerdings weist der EDSA nachdrücklich darauf hin, dass in einem solchen Fall den spezifischen Risiken dieses Szenarios auf andere Weise als durch Maßnahmen nach Kapitel V DS-GVO Rechnung getragen werden muss; sofern es sich beim Datenempfänger um einen Auftragsverarbeiter handelt, muss der Verantwortliche im Rahmen von Artikel 28 DS-GVO überprüfen, ob sein Auftragsverarbeiter die notwendige Zuverlässigkeit besitzt, die es gebietet, damit die Verarbeitung im Einklang mit der DS-GVO erfolgt. Zu den aus Art. 28 DS-GVO resultierenden Anforderungen in diesem Szenario hat sich im Übrigen im Berichtszeitraum auch die Konferenz der deutschen Datenschutzbehörden von Bund und Ländern geäußert (siehe dazu 10.2).

10.2 Extraterritoriale Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf Daten in der EU

Besondere datenschutzrechtliche Herausforderungen bestehen in Fällen, in denen Rechtsvorschriften von Drittländern dortigen Behörden die Möglichkeit geben, von Verantwortlichen oder Auftragsverarbeitern die Herausgabe personenbezogener Daten anzufordern, die in der Europäischen Union verarbeitet werden.

Spätestens mit dem Schrems-II-Urteil des Europäischen Gerichtshofs vom 16.07.2020 (C-311/18; siehe dazu unseren 11. Tätigkeitsbericht, Ziff. 10.1) ist für Unternehmen und andere Rechtsanwender deutlich geworden, dass die DS-GVO an Verarbeitungen personenbezogener Daten mit Drittlandsbezug hohe Anforderungen stellt. Eines der Kernprobleme sind dabei die Zugriffsmöglichkeiten von Behörden des Drittlands auf die übermittelten Daten. Eine Datenübermittlung ist nach der DS-GVO (unter anderem) nur zulässig, wenn solche Zugriffsmöglichkeiten das nach europäischem Recht zulässige Maß wahren (vgl. Ziff. 10.1 unseres 11. TB).

Im Berichtszeitraum wurden wir immer wieder mit Fällen konfrontiert, in denen rechtlich betrachtet zwar kein Fall einer Datenübermittlung in ein Drittland gegeben ist (zur Frage, wann dies der Fall ist, siehe auch Kapitel 10.1 dieses Tätigkeitsberichts), die Verarbeitung aber dennoch einen Drittlandsbezug im weiteren Sinne hat. Im Mittelpunkt stehen hier Fälle, in denen ein Verantwortlicher die Daten an einen Cloud-Dienstleister mit in einem Drittland (häufig: USA) ansässiger Muttergesellschaft gibt, wobei die Verarbeitung aber nicht durch die Muttergesellschaft erfolgt, sondern alleine durch eine europäische Tochtergesellschaft, die die Verarbeitung (nur) in der EU durchführt. Die Vergabekammer Baden-Württemberg hatte zunächst

in einem so gelagerten Fall eine Übermittlung in ein Drittland bejaht (Entscheidung vom 13.067.2022, Az. 1 VK 23/22), diese Entscheidung wurde indes später vom Oberlandesgericht Karlsruhe aufgehoben (Beschluss vom 07.09.2022, Az. 15 Verg 8/22). Nicht zuletzt dieser Fall war Anlass für die Konferenz der unabhängigen Datenschutzaufsichtsbehörden von Bund und Länder („Datenschutzkonferenz", DSK), sich mit diesem Szenario ausdrücklich zu befassen, um die Anwender:innen für ihre in solchen Fällen bestehenden datenschutzrechtlichen Pflichten zu sensibilisieren.

In ihrem Beschluss vom 31.01.2023 hält die DSK zunächst fest, dass die bloße Möglichkeit, dass eine Drittlands-Muttergesellschaft ihre EWR-Tochtergesellschaft anweisen könnte, oder dass eine öffentliche Stelle eines Drittlands unmittelbar ein EWR-Unternehmen anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln, für sich gesehen noch nicht dazu führt, dass schon die in der EU stattfindende Verarbeitung durch das EWR-Unternehmen eine Übermittlung in ein Drittland im Sinne von Artikel 44 DS-GVO darstellen würde. Jedoch kann, so die DSK, eine solche Gefahr dazu führen, dass dem als Auftragsverarbeiter eingesetzten EWR-Unternehmen die nach Artikel 28 Abs. 1 DS-GVO erforderliche Zuverlässigkeit fehlt. Daher muss der Verantwortliche bei der Prüfung der Zuverlässigkeit eines solchen Auftragsverarbeiters eine besonders hohe Sorgfalt walten lassen, die spezifisch dem Umstand möglicher Datenherausgabeanforderungen von Drittlandsbehörden oder seitens der EWR-Muttergesellschaft aus Anlass einer entsprechenden Anforderung einer Drittlandsbehörde Rechnung trägt. Die Datenschutzkonferenz fordert vom Verantwortlichen bei der Prüfung der Zuverlässigkeit eines solchen Auftragsverarbeiters eine Bewertung sämtlicher Umstände des Einzelfalls, wobei Prüfungsmaßstab stets die Frage ist, ob eine etwaige Anforderung zur Datenübermittlung in das Drittland die Maßstäbe der DS-GVO einhalten würde. Für den Maßstab der dem Verantwortlichen abverlangten Zuverlässigkeitsprüfung verweist die Datenschutzkonferenz auf das Papier „Empfehlungen 01/2020 des Europäischen Datenschutzausschusses", hält aber fest, dass die dortigen Maßstäbe für den Kontext von „echten" Datenübermittlungen in Drittländer getroffen wurden, so dass es hierbei nicht um eine komplette 1:1-Übertragung der Aussagen dieses Papiers geht, sondern vielmehr eine gemessen daran abweichende Bewertung im Einzelfall denkbar ist. Die DSK zählt eine Reihe von Gesichtspunkten auf, die der Verantwortliche bei der Zuverlässigkeitsprüfung typischerweise berücksichtigen sollte. Im Ergebnis wird der Verantwortliche sich bei der Prüfung seines Auftragsverarbeiters in solchen Fällen – obwohl rechtlich keine „Übermittlung in ein Drittland" vorliegt – stets vergewissern müssen, ob die dem Auftragsverarbeiter anvertrauten Daten zum Gegenstand infolge einer Herausgabeanforderung an eine Drittlandsbehörde werden könnten, die den nach europäischem Recht zulässigen Umfang überschreitet. Ist das der Fall, fehlt dem Auftragsverarbeiter die nach Art. 28 Abs. 1 DS-GVO erforderliche Zuverlässigkeit.

10.3 Prüfung der Vertragsdokumente von Microsoft 365 durch die DSK

Unter Leitung des Landesamts hat eine Arbeitsgruppe der Datenschutzkonferenz die dem Einsatz von Microsoft 365 zu Grunde liegenden allgemeinen Vertragsbindungen untersucht. Die Befunde der Arbeitsgruppe zeigen auf, dass vor allem für die im Vertrag vorbehaltenen Verarbeitungen personenbezogener Daten für eigene Zwecke des Auftragsverarbeiters zusätzliche Nachweise und Transparenzmaßnahmen erforderlich sind.

Vor dem Hintergrund zahlreicher Anfragen insbesondere zum Einsatz von Microsoft Teams für schulische Zwecke in mehreren Bundesländern

hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) in ihrer Sitzung vom 22. September 2020 eine Bewertung des Arbeitskreises Verwaltung zu den dem Einsatz des Produkts Microsoft Office 365 (jetzt: Microsoft 365) zu Grunde liegenden Online Service Terms (OST) sowie die Datenschutzbestimmungen für Microsoft-Onlinedienste (Data Processing Addendum / DPA) — Stand: Januar 2020 — hinsichtlich der Erfüllung der Anforderungen von Artikel 28 Absatz 3 Datenschutz-Grundverordnung (DS-GVO) zur Kenntnis genommen. Die damalige Bewertung des Arbeitskreises kam zum Ergebnis, „dass auf Basis dieser Unterlagen kein datenschutzgerechter Einsatz von Microsoft Office 365 möglich" sei.

Die DSK hatte daraufhin eine eigene Arbeitsgruppe unter Federführung Brandenburgs und des BayLDA als für den Deutschlandsitz des Herstellers zuständige Behörde gebeten, Gespräche mit dem Hersteller aufzunehmen, „um zeitnah datenschutzgerechte Nachbesserungen sowie Anpassungen an die durch die Schrems II-Entscheidung des EuGH aufgezeigten Maßstäbe an Drittstaatentransfers für die Anwendungspraxis öffentlicher und nicht öffentlicher Stellen zu erreichen".

Auf Grundlage eines mittlerweile öffentlich zugänglichen Abschlussberichts dieser Arbeitsgruppe hat die DSK am 24. November 2022 einstimmig folgenden Beschluss gefasst:

„Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten „Datenschutznachtrags vom 15. September 2022" nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden."

Zusätzlich zu der ausführlichen Darstellung der Untersuchungsergebnisse steht eine Zusammenfassung der Kernbefunde der Arbeitsgruppe zur Verfügung. Die Untersuchungen behandeln mit Fragestellungen u.a. zur Reichweite eigenständiger Verarbeitungsbefugnisse des Auftragsverarbeiters, zur Zweckänderung oder den Auswirkungen extraterritorialer Zugriffsrechte (siehe hierzu bereits Kapitel 10.2) zahlreiche auch losgelöst von den vertraglichen Regelungen zu Microsoft 365 in der aufsichtlichen Praxis wiederkehrende Problemfelder. Sie können insoweit für die Datenschutzpraxis auch für weiterführende Analysen herangezogen werden.

Parallel zu dem Prüfprojekt der DSK haben im Berichtszeitraum im Übrigen koordiniert durch den Europäischen Datenschutzausschuss mehrere europäische Datenschutzaufsichtsbehörden gemeinsame Untersuchungen zum Einsatz von Cloud-Diensten im öffentlichen Bereich durchgeführt. Der Abschlussbericht macht deutlich, dass die in den Untersuchungen der DSK-Arbeitsgruppe identifizierten Prüf- und Kritikpunkte letztlich typische Datenschutzkonflikte beim Einsatz von Cloud-Anwendungen zahlreicher Anbieter unterschiedlicher Ausrichtung und Herkunftsländer darstellen und daher regelmäßig besondere Aufmerksamkeit der datenschutzrechtlich Verantwortlichen verlangen.

10.4 Follow Up zum Einsatz von Google Analytics

Die Übermittlung personenbezogener Daten in Drittländer im Rahmen des Einsatzes von Google Analytics verstößt gegen die Anforderungen des V. Kapitels der DS-GVO, soweit dabei eindeutige Kennungen übermittelt werden.

Bereits unter Nr. 5.2 unseres Tätigkeitsberichts für 2021 haben wir unsere aufsichtliche Bewertung der beim Einsatz des weit verbreiteten Tools Google Analytics stattfindenden Verarbeitungen personenbezogener Daten dargestellt. Die Bewertung bezog sich auf die dort näher beschriebene Gestaltung, bei der (in Cookies enthaltene) einzigartige Kennungen (IDs) auf den Nutzerrechner gesetzt werden, die gemeinsam mit einer Reihe von Informationen über das Nutzersystem aus dem Browser des Nutzers an Google übermittelt werden, so dass der Nutzerrechner von anderen Rechnern unterschieden und damit „wiedererkannt" werden kann. Nach unserer im Tätigkeitsbericht 2021 dargestellten Bewertung, die auch von zahleichen anderen europäischen Datenschutzaufsichtsbehörden geteilt wurde, lag darin eine Übermittlung personenbezogener Daten unter Verstoß gegen die Anforderungen des fünften Kapitels der DS-GVO.

In der Zwischenzeit haben weitere europäische Aufsichtsbehörden Anordnungen gegen Websitebetreiber in mehreren weiteren EU-Mitgliedstaaten erlassen oder Äußerungen getätigt, in denen sie sich dieser datenschutzrechtlichen Bewertung angeschlossen haben (siehe etwa den Bescheid der italienischen Aufsichtsbehörde vom 09.06.2022, Pressemitteilung der dänischen Datenschutzaufsichtsbehörde vom 21.09.2022,) und in einigen Fällen den betreffenden Websitebetreibern den Einsatz des Tools in der oben genannten Gestaltung untersagt.

Wie bereits im Tätigkeitsbericht 2021 berichtet hat Google – soweit erkennbar im September 2021 - die für den Einsatz der sog. Google Werbeprodukte (Google Ads), darunter von Google Analytics, seinen den Kunden angebotenen Auftragsverarbeitungsvertrag abgeändert. Dabei wurden insbesondere die neuen – im Juni 2021 veröffentlichten - Standardvertragsklauseln der Europäischen Kommission für Datenübermittlungen in Drittländer in den Auftragsverarbeitungsvertrag für Google Werbeprodukte aufgenommen (siehe die aktuelle Fassung dieses Auftragsverarbeitungsvertrags, Stand 01.01.2023; https://business.safety.google/adsprocessorterms/, dort Ziffer. 10.2). Google gibt zudem an, eine Reihe von sog. Zusätzlichen Maßnahmen (supplementary measures; veröffentlicht unter https://business.safety.google/adsprocessorterms/) zu ergreifen, mit denen es der Auffassung ist, das nach Kapitel V der DS-GVO für Drittlandsübermittlungen geforderte Schutzniveau zu gewährleisten.

Trotz dieser Änderungen gilt aus unserer Sicht unverändert: Soweit Websitebetreiber Google Analytics in Varianten einsetzen, bei denen eindeutige Kennungen (IDs) an Google-Server in die USA übermittelt werden, verstoßen sie nach wie vor gegen Kapitel V der DS-GVO. Die o.g. von Google angebotenen „zusätzlichen Maßnahmen" führen nach unserer Bewertung zu keinem anderen Ergebnis, da durch sie eine Übermittlung personenbezogener Daten an Google-Server in den USA nicht ausgeschlossen wird. Auch dass in der Variante „Google Analytics 4" jedenfalls nach Angaben von Google zumindest in aller Regel keine IP-Adressen mehr an US-Server übermittelt werden, führt zu keiner anderen Bewertung, sofern die auf den Rechner des Nutzers gesetzten eindeutigen Kennungen und damit personenbezogene Daten an US-Server übermittelt werden. Diese Rechtsauffassung haben wir im Rahmen mehrerer von uns geführter Vorgänge gegenüber den betreffenden Websitebetreibern kommuniziert. Der Erlass förmlicher Anordnungen war in den von uns geführten Verfahren nicht notwendig, weil die Betreiber den Einsatz nach unserem Hinweis jeweils beendet haben.

Eine mögliche „Lösung", um Verstöße gegen Kapitel V der DS-GVO beim Einsatz von Google Analytics zu vermeiden, hat die französische Aufsichtsbehörde am 20.06.2022 mit Blick auf eine Einsatzvariante unter Nutzung eines Proxy

Servers aufgezeigt . Den Ausführungen der französischen Aufsichtsbehörden stimmen wir zu. Bei der dort aufgezeigten Einsatzvariante wird ein direkter Datenfluss zwischen dem Nutzerrechner und Servern von Google durch Zwischenschaltung eines Proxy-Servers unterbunden. Letztlich erfolgt dabei vor der Übermittlung von Daten an Google-Server eine Pseudonymisierung. Ein datenschutzkonformer Einsatz ist dabei jedoch von einer Reihe von Bedingungen abhängig. Entscheidend ist, ob es im Einzelfall gelingt sicherzustellen, dass die pseudonymisierten Daten, die an Google übermittelt werden, von Google nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden können. Grundvoraussetzung hierfür ist, dass auf dem Proxy-Server jegliche eindeutigen Kennungen entfernt werden und darüber hinaus auch alle weiteren Informationen, die im Falle ihrer Übermittlung an Google-Server zu einer Unterscheidbarkeit des einzelnen Nutzerrechners von anderen Nutzern führen könnten. Ob dies gelingt, kann letztlich nur im Einzelfall bewertet werden (Näheres zu den Kriterien unter der o.g. Veröffentlichung der französischen Datenschutzbehörde).

11

Beschäftigtendatenschutz

11 Beschäftigtendatenschutz

11.1 Anforderung einer Kopie des Personalausweises zur eindeutigen Identifizierung zwei Monate nach Eingang des Auskunftsbegehrens

Auch das Nachfordern weiterer Daten zur eindeutigen Identifizierung der betroffenen Person muss innerhalb der Monatsfrist des Art. 12 Abs. 3 S. 1 DS-GVO erfolgen. Grundsätzlich ist dabei eine Kopie des Personalausweises nicht erforderlich, sondern es sind weitere Personalstammdaten wie Geburtsdatum und Adresse ausreichend.

Auch im Beschäftigungskontext erhielten wir im Berichtszeitraum Eingaben zu Betroffenenrechten gem. Art. 12 ff. DS-GVO.

Beispielsweise erhielten wir von einem ehemaligen Arbeitnehmer folgende Beschwerde:
Der Mitarbeiter begehrte von seinem Arbeitgeber nach seinem Ausscheiden per E-Mail Auskunft gemäß Art. 15 DS-GVO zu den zu seiner Person gespeicherten Daten. Er erhielt eine automatische Antwort über den Eingang der E-Mail. Nach zwei Monaten erhielt er eine Antwort von seinem Arbeitgeber. Dieser wies darauf hin, dass die Übermittlung der Auskunft an eine falsche Person erhebliche Auswirkungen auf den Betroffenen haben könne. Er führe deshalb vor Erfüllung des Auskunftsbegehrens eine eindeutige Identifizierung der betroffenen Person durch. Die vom Betroffenen mitgeteilten Legitimationsdaten würden nicht mit den dem Arbeitgeber zur Verfügung stehenden Daten übereinstimmen. Um die bestehenden Zweifel und die Legitimationsprüfung durchführen zu können, bat der Arbeitgeber um eine Kopie des Personalausweises.

Gemäß Art. 12 Abs. 3 S. 1 DS-GVO hat der Verantwortliche dem Betroffenen die Informationen u.a. bei einem Auskunftsbegehren unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags, zur Verfügung zu stellen. Aber auch, wenn der Verantwortliche gem. Art. 12 Abs. 6 DS-GVO weitere Informationen zur Identifizierung anfordert, muss dies unverzüglich und spätestens innerhalb der Monatsfrist geschehen, da die betroffene Person in jedem Fall innerhalb der Monatsfrist eine Reaktion des Verantwortlichen erwarten darf. Werden weitere Informationen zur Identifizierung angefordert, wird die Frist bis zu dem Zeitpunkt, in dem alle Informationen vorliegen, ausgesetzt. Die automatische Antwort in der dargestellten Beschwerde besagte, dass das Auskunftsbegehren beim Arbeitgeber an diesem Tage eingegangen war, mit der Folge, dass die nach zwei Monaten erteilte Reaktion deutlich verspätet war. Um einen Abgleich und eine Identifizierung vornehmen zu können, hätte es in dem geschilderten Fall ausgereicht, weitere Stammdaten zum Abgleich anzufordern, z.B. Geburtsdatum und Adresse. Die Forderung nach Vorlage einer Kopie des Personalausweises war nicht erforderlich, damit unverhältnismäßig und stand darüber hinaus nicht im Einklang mit den Vorgaben des § 20 Abs. 2 Personalausweisgesetz.

11.2 Kontrolle von Beschäftigten im Homeoffice

Kontrolle von Beschäftigten im Homeoffice ist nur eingeschränkt.

Im Berichtszeitraum erreichten uns vermehrt Anfragen zum Thema „Arbeiten im Homeoffice“. Hierbei ging es häufig darum, zu erfahren, inwieweit eine Überprüfung der Beschäftigten im Homeoffice aus datenschutzrechtlicher Sicht erlaubt ist. Die Nachfragen zielten zum ei-

nen darauf ab, festzustellen, ob sich die Beschäftigten an die vereinbarten Rahmenbedingungen (örtlich, zeitlich) halten und inwieweit diese ihren arbeitsvertraglichen Pflichten nachkommen.

Zu der Frage, ob eine GPS-Überwachung zur Überprüfung, ob von dem vereinbarten Arbeitsort aus gearbeitet wird, haben wir uns dahingehend geäußert, dass wir eine stichprobenartige Kontrolle der Anwesenheit am Arbeitsplatz zu Hause bzw. an dem vereinbarten Ort auch mittels GPS auf Grundlage des Art. 6 Abs. 1 Buchst. b DS-GVO[1] jedenfalls unter nachstehenden Maßgaben als begründbar ansehen:
Aufgrund des erheblichen Missbrauchspotentials einer GPS-Ortung, sind im Rahmen der Erforderlichkeit etwaige mildere Maßnahmen zu prüfen. So könnte beispielsweise ein „Kontrollanruf" auf der heimischen Festnetznummer in Betracht kommen. Als Rechtsgrundlage für diese Datenverarbeitung wäre ebenfalls Art. 6 Abs. 1 Buchst. b DS-GVO[2] einschlägig; auch hier sind die Betroffenen gem. Art. 13 DS-GVO zum Zeitpunkt der Datenerhebung über die Datenverarbeitung zu informieren.
Soweit eine private Festnetznummer bereits vorliegt, liegt in der Verwendung der Telefonnummer zur Durchführung von Stichprobenkontrollen eine Zweckänderung vor, vgl. § 24 BDSG, Ausübung zivilrechtlicher (arbeitsrechtlicher) Ansprüche, ggf. Art. 6 Abs. 4 DS-GVO. Auch hier besteht gem. Art. 13 Abs. 3 DS-GVO eine Informationspflicht vor Weiterverarbeitung für den anderen Zweck.
Aufgrund des Rechts auf Unverletzlichkeit der Wohnung ist eine Kontrolle vor Ort, zumindest dann, wenn die Wohnung des Beschäftigten betreten werden sollten, kritisch zu sehen. In diesem Zusammenhang haben wir auch auf die Ausführungen in der Veröffentlichung des Bundesbeauftragen für Datenschutz und Informationsfreiheit, Telearbeit und Mobiles Arbeiten, S. 18 f. (abrufbar unter Telearbeit und Mobiles Arbeiten (bund.de)) verwiesen.
Mittels technisch-organisatorische Maßnahmen ist gem. Art. 32 sicherzustellen, dass ein Zugriff auf die GPS-Daten tatsächlich nur zu einer solcher Kontrolle zum Zeitpunkt der Kontrolle von zuvor bestimmten Personen (Zugriffsberechtigung) während der Arbeitszeit stattfindet. Weiterhin sind die Beschäftigten über die Möglichkeit der GPS-Ortung (ggf. Installation entsprechender Programme, den Zugriff hierauf und der Rahmenbedingungen für einen Zugriff zu informieren, Art. 13 DS-GVO.
Die Häufigkeit der Stichprobenkontrollen muss sich dabei an der Erforderlichkeit und Verhältnismäßigkeit messen lassen. Grundsätzlich wird zudem ein Live-Zugriff während der regulären Arbeitszeit ausreichen, so dass es keiner dauerhaften Protokollierung der Aufenthaltsorte bedarf.

Soweit ein begründeter Verdacht für eine Straftat oder schwere Pflichtverletzung gegeben ist, muss sich die Datenverarbeitung an Art. 6 Abs. 1 Buchst. b DS-GVO[3] messen lassen. In diesem Fall kann ein Protokollieren für einen bestimmten Zeitraum und die Einsichtnahme in ein begrenztes Bewegungsprofil, das also nicht über die Aufzeichnung der Anwesenheit am Heimarbeitsplatz während der Dienstzeit hinausgeht, begründbar sein.

Den Einsatz von Keylogger-Anwendungen zur Prüfung der Produktivität bzw. der Kontrolle der tatsächlichen Tätigkeit oder inwieweit konkrete Programme genutzt werden ohne einen auf konkrete Tatsachen gegründete Verdacht zumindest einer schwerwiegenden Pflichtverletzung ist in der Regel nicht zulässig. Mittels Keylogger-Anwendungen können jegliche Eingaben protokolliert werden, so dass ein umfangreiches Bild der Tätigkeiten, die mit dem ent-

[1] Im Lichte der EuGH-Rechtsprechung in der Rechtssache C-34/21 sehen wir § 26 Abs. 1 S. 1 BDSG nicht für anwendbar an.

[2] Vgl. Fn. 1.

[3] Vgl. Fn. 1.

sprechenden Gerät durchgeführt werden, erstellt werden kann, da es möglich ist, zu erfassen sowie zu erkennen, was konkret eingegeben (u.a. Passwörter, Nachrichteninhalte) wurde. Soweit Einstellungen bei der Keylogger-Anwendung so gesetzt werden, dass z.B. nur noch ein Tastenanschlag oder eine Mausbewegung erkannt wird, stellt sich jedoch insbesondere die Frage nach der Eignung, da lediglich festgestellt werden könnte, dass ein Tastaturanschlag erfolgt, jedoch nicht durch wen und ob dabei eine Tätigkeit durchgeführt wird. Gleiches gilt, wenn eine stichprobenmäßige Kontrolle der genutzten Programme erfolgen soll. Ein:e Beschäftigte:r ist oftmals frei darin, ihre/seine Arbeitszeit einzuteilen und es kommt häufig auf die Arbeitsergebnisse, die (fristgebunden) vorliegen müssen, an. Inwieweit die Kenntnis, dass zu einem bestimmten Zeitpunkt bzw. in einem bestimmten begrenzten Zeitraum ein bestimmtes Programm genutzt wurde, Erkenntnisse darüber liefert, was ein:e Beschäftigte:r macht, müsste konkret dargestellt und nachgewiesen werden.

11.3 Was uns während der Corona-Pandemie beschäftigt hat und welches Fazit wir ziehen

Information und die konsequente Anwendung datenschutzrechtlicher Regelungen geben auch in dynamischen Geschehen Orientierung.

Insbesondere in der ersten Hälfte des Berichtszeitraumes haben wir uns im Bereich Beschäftigtendatenschutz mit zahlreichen Fragestellungen betreffend die Datenverarbeitung im Zusammenhang mit der Corona-Pandemie beschäftigt.

3G-Zugangsregelung, § 28b IfSG a.F.

Die Anfragen und Eingaben betrafen insbesondere den bereits Ende des Jahres 2021 in Kraft getretenen § 28b IfSG a.F. und die darin geregelte 3G-Regelung am Arbeitsplatz. § 28b Abs. 1 und 3 IfSG a.F. (ab 24.11.2021 BGBl. I S.4906) bestimmten insbesondere, dass Arbeitsstätten, bei denen physische Kontakte nicht ausgeschlossen werden konnten, nur mit einem G-Nachweis (Test-, Genesenen- oder Impfnachweis) betreten werden durften bzw. es musste unmittelbar in der Arbeitsstätte ein Test- oder Impfangebot der/des Arbeitgeber:innen wahrgenommen werden. Den Arbeitgeber:innen wurde eine Überwachungs- und Dokumentationspflicht auferlegt :

> (1) Arbeitgeber und Beschäftigte dürfen Arbeitsstätten, in denen physische Kontakte von Arbeitgebern und Beschäftigten untereinander oder zu Dritten nicht ausgeschlossen werden können, nur betreten und Arbeitgeber dürfen Transporte von mehreren Beschäftigtn zur Arbeitsstätte oder von der Arbeitsstätte nur durchführen, wenn sie geimpfte Personen, genesene Personen oder getestete Personen (...) einen Impfnachweis, einen Genesenennachweis oder einen Testnachweis (...) mit sich führen, zur Kontrolle verfügbar halten oder bei dem Arbeitgeber hinterlegt haben. (...). Abweichend von Satz 1 ist Arbeitgebern und Beschäftigten ein Betreten der Arbeitsstätte erlaubt, um
>
> 1. unmittelbar vor der Arbeitsaufnahme ein Testangebot des Arbeitgebers zur Erlangung eines Nachweises (...) wahrzunehmen oder
> 2. ein Impfangebot des Arbeitgebers wahrzunehmen.
>
> (...)
>
> (3) Alle Arbeitgeber (...) sind verpflichtet, die Einhaltung der Verpflichtungen nach Absatz 1 Satz 1 (..) durch Nachweiskontrollen täglich zu überwachen und regelmäßig zu dokumentieren. Alle Arbeitgeber und jeder Beschäftigte sowie Besucher der in Absatz 2 Satz 1 ge-

> nannten Einrichtungen und Unternehmen sind verpflichtet, einen entsprechenden Nachweis auf Verlangen vorzulegen. Soweit es zur Erfüllung der Pflichten aus Satz 1 erforderlich ist, darf der Arbeitgeber (…) zu diesem Zweck personenbezogene Daten einschließlich Daten zum Impf-, Sero- und Teststatus in Bezug auf die Coronavirus-Krankheit-2019 (COVID-19) verarbeiten. (…). § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend. Die zuständige Behörde kann von jedem Arbeitgeber (…) die zur Durchführung ihrer Überwachungsaufgabe erforderlichen Auskünfte verlangen. (…) Die nach Satz 3 (…) erhobenen Daten sind spätestens am Ende des sechsten Monats nach ihrer Erhebung zu löschen; die Bestimmungen des allgemeinen Datenschutzrechts bleiben unberührt.

Insbesondere konnten wir bei Arbeitgeber:innen und Beschäftigten eine erhebliche Verunsicherung bezüglich des Umfangs der erforderlichen Datenverarbeitungsbefugnis aus § 28b Abs. 3 S. 3 IfSG a.F. wahrnehmen, die mit der Änderung der COVID-19-Schutzmaßnahmen-Ausnahmenverordnung (SchAusnahmV) vom 14.01.2022 und den geänderten Anforderungen an die Gültigkeit von Genesenen- und Impfzertifikaten nochmals verstärkt wurde. Dies führte dazu, dass den Arbeitgeber:innen teilweise weitreichende Datenverarbeitungen, insbesondere Speicherungen empfohlen wurden, um für jegliche behördliche Kontrolle und künftige Änderungen der Anforderungen an G-Nachweise „gewappnet" zu sein. Die Arbeitgeber:innen standen bei den bei uns eingehenden Anfragen und Eingaben oftmals vor dem Dilemma, sicherheitshalber für den Fall einer Überprüfung der Einhaltung der 3G-Regelung mit für sie nicht abschätzbarer Kontrolltiefe zahlreiche personenbezogene Daten und insbesondere Gesundheitsdaten zu verarbeiten oder aber im Gegensatz dazu möglichst wenige Daten zu verarbeiten und einem etwaigen Risiko ausgesetzt zu sein, dass die Durchführung der Kontrollen nicht ausreichend nachgewiesen werden könnten.

Neben dem „Zuviel" an Datenverarbeitung stellten wir in Beschwerdeverfahren aber auch ein „an zu viele Personen" fest, das heißt Verstöße gegen Art. 5 Abs.1 a DS-GVO, § 28b Abs. 3 Satz 3 IfSG a.F. sowie Art. 5 Abs. 1 f DS-GVO, § 28 b Abs. 3 S. 5 IfSG a.F., § 22 Abs. 2 Nr. 5 BDSG entspr., da eine unzulässige Offenbarung gespeicherter G-Nachweise an unberechtigte Personen erfolgte und eben eine entsprechende Zugriffsbeschränkung innerhalb des Unternehmens weder geregelt noch umgesetzt worden war.

Sowohl die Datenschutzkonferenz (https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf, dort Frage und Antwort Nr. 8), als auch wir, haben die gesetzliche Regelungen datenschutzrechtlich mittels Anwendungshinweisen bzw. FAQs bewertet.

Nachdem die bundesweite und alle Beschäftigten treffende 3G-Zugangsregelung des § 28b IfSG a.F. mit Ablauf des 19. März 2022 außer Kraft getreten ist, waren dann aber jegliche Dokumentationen sowie Kopien von G-Nachweisen zu löschen, soweit nicht eine anderweitige Rechtsgrundlage zur Verarbeitung derselben vorlag.

Im Anschluss erreichten uns zahlreiche Anfragen dahingehend, ob Arbeitgeber: innen insbesondere gestützt auf das Hausrecht selbst eine 3G-Zugangsregelung für die eigenen Beschäftigten vorgeben können. Eine gesetzliche Grundlage dafür, dass dies pauschal und für alle Beschäftigten möglich war, konnten wir nicht erkennen. Allenfalls sahen wir bei Vorliegen der Voraussetzungen zur Erstellung eines Hygienekonzepts oder im Rahmen des Direktionsrechts der Arbeitgeber:innen zur Erfüllung der Schutzpflichten der Arbeitgeber:innen gem. § 618 Abs. 1 BGB und § 3 Abs. 1 S. 1 ArbSchG in eng be-

grenzten Konstellationen die Vorgabe zur Erbringung eines Testnachweises (mit der Möglichkeit sich von dieser mittels Nachweises des Vorliegens eines vollständigen Impfschutzes/ eines Genesenenstatus) begründbar.

Einrichtungsbezogene Impfpflicht, § 20a IfSG a.F.

Neben der bundesweit geregelten 3G-Zugangskontrolle von Beschäftigten erreichten uns zudem Beratungsanfragen und Eingaben bezüglich der Regelung in § 20a IfSG a.F., wonach Personen, die in bestimmten Einrichtungen oder Unternehmen tätig waren, ab dem 15.03.2022 (geltenden Fassung vom 12.12.2021 mit weiteren Änderungen in der geltenden Fassung vom 19.03.2022 bzw. vom 17.09.2022) einen Immunitätsnachweis (Impf- bzw. Genesenennachweis) bzw. ein Zeugnis, dass sie aufgrund einer medizinischen Kontraindikation nicht gegen das Coronavirus SARS-CoV-2 nicht geimpft werden konnte, vorlegen mussten. Insbesondere ging es um die Fragestellung, ob bereits in Vorbereitung auf die Verpflichtung ab dem 15.3.2022 geimpft oder genesen zu sein, die entsprechenden G-Nachweise von der Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens verlangt werden dürften, ob hiervon Kopien angefertigt werden dürften, welcher Personenkreis von der Regelung umfasst ist und ob Beschäftigte, die keinen Nachweis oder kein Zeugnis vorlegen, zu Gesprächen geladen werden dürften. Wiederum wurde seitens der Datenschutzkonferenz ein Beschluss zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht veröffentlicht, auf die hier verwiesen wird (https://www.datenschutzkonferenz-online.de/media/dskb/2022_13_04_beschluss_DSK_20a_IfSG.pdf).

Der Großteil der Beschwerden, die wir im Zusammenhang mit der Regelung in § 20a IfSG a.F. erhielten, richtete sich gegen die Weitergabe von personenbezogenen Daten im Rahmen der Meldung der verpflichteten Einrichtung bzw. des verpflichteten Unternehmens bei einer Nichtvorlage oder bei Zweifeln an der Echtheit an das zuständige Gesundheitsamt.

Auch bezüglich der aufgrund der vorgenannten Regelung verarbeiteten personenbezogenen Daten war eine Löschung spätestens mit Ablauf der Rechtsgrundlage am 31. Dezember 2022 vorzunehmen, da § 20a IfSG zu diesem Zeitpunkt außer Kraft trat.

Entschädigung, § 56 IfSG a.F.

Weiterhin beschäftigte uns die Frage, ob Arbeitgeber:innen im Zusammenhang mit der Antragstellung auf Erstattung nach § 56 Abs. 5 S. 1 IfSG („Bei Arbeitnehmern hat der Arbeitgeber für die Dauer des Arbeitsverhältnisses, längstens für sechs Wochen, die Entschädigung für die zuständige Behörde auszuzahlen.“) zu empfehlen ist, das negative Testergebnis eines Arbeitnehmers zu dokumentieren bzw. zu den Unterlagen zu nehmen, welches das einen Entschädigungsanspruch nach § 56 Abs. 1 IfSG begründendes Tätigkeitsverbot beendet. Ziffer 5 der damals geltenden Allgemeinverfügung Isolation des BayStMGP vom 12.04.2022 beinhaltete eine Regelung zur Wiederaufnahme der Beschäftigung nach Beendigung der Isolation für Beschäftigte in Einrichtungen nach § 23 Abs. 3 Satz 1, Abs. 5 Satz 1 und § 36 Abs. 1 Nr. 2, 7 IfSG, d.h. sie betraf nur bestimmte Beschäftigte. Diese mussten bei Wiederaufnahme der Tätigkeit ihrer/ihrem Arbeitgeber:in ein negatives Antigen- oder PCR-Testergebnis oder aber ein positives Testergebnis mit einem ct-Wert größer 30 vorlegen.
Wir sahen die Dokumentation der Vorlage eines Negativergebnisses bzw. eines Ergebnisses ct-Wert größer 30 dann, wenn gem. § 56 IfSG hinsichtlich (vormals positiv getesteter) Beschäftigter in Einrichtungen nach § 23 Abs. 3 Satz 1, Abs. 5 Satz 1 und § 36 Abs. 1 Nr. 2, 7 IfSG eine Entschädigung durch den Arbeitgeber beantragt werden sollte, auf Grundlage des § 26 Abs.1, 3

BDSG als begründbar an. Zur Erfüllung rechtlicher Pflichten aus dem Recht der sozialen Sicherheit war es erforderlich, dass Arbeitgeber:innen den konkreten Zeitraum bei Antragstellung benennen konnte und zudem dokumentiert hatte, dass die hierfür erforderliche Vorlage an die/den Arbeitgeber:in durch die/den Beschäftigte:n erfolgte.

Verarbeitung der Information über Corona-Infektion

Arbeitgeber:innen fragten sich außerdem, inwieweit und auf welcher Grundlage die Information, dass eine Infektion mit dem SARS-CoV-2-Virus bei einer/m Beschäftigten vorlag, genutzt werden durfte, um etwaige Kontakte über ein mögliches Infektionsrisiko zu informieren. Soweit die Kontakte einer/s positiv getesteten Beschäftigten von dieser/m nicht oder nicht zeitnah benannt werden könnte, werteten wir regelmäßig eine Information, dass es in bestimmten Räumlichkeiten oder in bestimmten Besprechungen zu einer Kontaktsituation gekommen sein konnte, als ausreichend an.
Je nach konkreter Situation und nur in ganz bestimmten Einzelfällen sahen wir die Möglichkeit einer namentlichen Nennung einer/s infizierten Beschäftigten auf der Grundlage des § 26 Abs. 1, 3 BDSG als zulässig an. Aber auch hierbei forderten wir stets zu prüfen, ob die Nennung erforderlich war, an welchen Kreis der Name offenbart werden sollte und dass insbesondere angemessene Maßnahmen gem. § 22 Abs. 2 BDSG getroffen werden.

Fazit

An verschiedenen Stellen hätten wir uns zwar gewünscht, dass von etwaigen Verordnungsermächtigungen zur Konkretisierung gesetzlicher Regelungen (umfassender) Gebrauch gemacht worden wäre, sahen aber sowohl den Gesetzgeber und die Verwaltung – so auch uns – in der Pflicht, Bewertungen und Anforderungen klar zu kommunizieren. Diese Kommunikation geschah vielerorts in entsprechenden Online-Veröffentlichungen, insbesondere durch FAQs.

Daneben mussten wir aber auch in der Bearbeitung von Anfragen und Eingaben im Berichtszeitraum immer wieder feststellen, dass die jeder Datenverarbeitung zugrunde liegenden und zu beachtenden Grundsätze des Art. 5 DS-GVO nicht konsequent beachtet und die Einhaltung derselben nicht immer geprüft wurde. Gerade mit den Grundsätzen der Zweckbindung, der Datenminimierung und der Speicherbegrenzung konnte bereits Orientierung bezüglich zahlreicher Fragestellungen gefunden werden.

Unser Fazit, welches wir in datenschutzrechtlicher Hinsicht insbesondere auch aus der Corona-Pandemie ziehen können, ist, dass gerade dann, wenn bei einer großen Dynamik im Geschehen und in der Gesetzgebung zahlreiche datenschutzrechtliche Unsicherheiten bestehen, einerseits eine schnelle und breit gefächerte Kommunikation erforderlich ist und die Besinnung auf die datenschutzrechtlichen Grundsätze Orientierung und Sicherheit bezüglich der durchzuführenden Datenverarbeitungen geben kann.

11.4 Forderung nach Schaffung eines eigenständigen Beschäftigungsdatenschutzgesetzes

Beschäftigtendatenschutz muss praktikabel, normenklar und sachgerecht sein.

Die Datenschutzkonferenz hat im Berichtszeitraum die Ankündigungen im Koalitionsvertrag der 20. Legislaturperiode, der das Ziel der Schaffung von Regelungen zum Beschäftigtendatenschutz, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen, formuliert, zum Anlass genommen sich im April 2022 zu der

Notwendigkeit über die derzeitigen Regelungen hinausgehende Regelungen mit dem Ziel der Normenklarheit und damit Rechtssicherheit zu schaffen (DSK-Entschließung vom 29.04.2022 „Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt"!", abrufbar unter https://datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf).

Damit wird den bestehenden Forderungen nach Schaffung eines umfassenden und eigenständigen Beschäftigtendatenschutzgesetzes, die darauf abzielen, gerade im digitalen Zeitalter eine Festsetzung gesetzlicher Standards zu erreichen um die Rechtssicherheit für Arbeitgeber:innen zu erhöhen und einen wirksamen Grundrechtsschutz für Beschäftige zu schaffen, Nachdruck verliehen.

Der Gesetzgeber selbst hatte sich bei Erlass des § 26 BDSG weitergehende Regelungen des Beschäftigtendatenschutzes ausdrücklich vorbehalten. Dieses Ziel wurde dann auch im Koalitionsvertrag der 19. Legislaturperiode mit Blick auf die Spezifizierungsmöglichkeiten, die Art. 88 DSGVO gewährt, formuliert. Ein in der Folge durch das Bundesministerium für Arbeit und Soziales eingesetzter unabhängiger, interdisziplinärer Beirat zum Beschäftigtendatenschutz kam hinsichtlich der Frage, ob ein eigenständiges Gesetz zum Beschäftigtendatenschutz, das die Persönlichkeitsrechte der Beschäftigten am Arbeitsplatz schützt und Rechtssicherheit für den Arbeitgeber schafft, erlassen werden sollte, ebenfalls zu dem Ergebnis, dass ein rechtssicherer und dadurch wirksamer Datenschutz im Beschäftigungskontext gerade im digitalen Zeitalter gefordert ist.

Auf Grund der nunmehr am 30.03.2023 ergangenen EuGH-Entscheidung zur europarechtskonformen Umsetzung des Beschäftigtendatenschutzrechts in Hessen wurde der Überprüfungs- und Handlungsbedarf im Bereich des Beschäftigtendatenschutzrechts sichtbar (Rechtssache C-34/21), da die Vorschrift des § 23 Abs. 1 HDSIG ist in ihrem Wortlaut mit § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) weitgehend identisch ist.

In der Konsequenz bedarf es einerseits einer Überprüfung dahingehend, ob die nationalen Regelungen sowie Kollektivvereinbarungen von der Spezifizierungsklausel des Art. 88 DS-GVO gedeckt sind bzw. die nationale Regelung im Zusammenhang mit anderen Öffnungsklauseln unionsrechtskonform sind. Andererseits bedarf es seitens des Gesetzgebers einer Überprüfung, inwieweit von der Spezifizierungsklausel gem. Art. 88 DS-GVO künftig dahingehend Gebrauch gemacht wird, dass spezifischere Regelungen erlassen werden, die auch den Anforderungen des Art. 88 Abs. 2 DS-GVO gerecht werden.

12

Gesundheit und Soziales

12 Gesundheit und Soziales

12.1 Diskretion bei der Anmeldung und im Sprechzimmer

Auf Grund fehlender oder mangelhafter Diskretion werden Patient:innendaten in Praxen von Leistungserbringern in unzulässiger Weise gegenüber Dritten offengelegt. Ärzt:innen legen so unzulässig besonders sensible Daten ihrer Patient:innen offen.

Gespräche an der Anmeldung, bei denen Gesundheitsdaten in Verbindung mit Name und Geburtsdatum abgefragt werden, sollten nicht von anderen wartenden Patient:innen mitgehört werden können. Auch dürfen an den Anmeldungen Arztverordnungen und Patientenunterlagen nicht so abgelegt werden, dass diese von anderen Patient:innen eingesehen werden können. In einer Physiotherapiepraxis wurden Arztverordnungen sogar bewusst dort ausgelegt, um Unterschriften der Patient:innen einzuholen. Die Anmeldung war währenddessen nicht vom Praxispersonal besetzt, sodass seitens der Arztpraxis auch nicht kontrolliert wurde, welche Patient:innen worauf Zugriff nehmen. Als einen gravierenden Verstoß werten wir, wenn die in den Sprechzimmern vorhandenen PCs nicht gesperrt werden, sodass darin wartende Patient:innen Einblick in die Akte der zuvor behandelten Person und allgemeinen Zugriff auf das Programm zur Führung der Patientenakten nehmen können.

Das Sperren von PCs bei Verlassen des Arbeitsplatzes bzw. Schreibtisches muss als Selbstverständlichkeit vom gesamten Praxispersonal umgesetzt werden. Die Anmeldung und das Wartezimmer sollten, soweit es die baulichen Gegebenheiten dies zulassen, räumlich voneinander getrennt sein, sodass Gespräche an der Anmeldung nicht einhörbar sind. Ist das nicht möglich, sollten entsprechende bauliche Ergänzungen umgesetzt werden und Gespräche sowie Telefonate über sensible Daten alternativ in einem separaten Zimmer geführt werden. Zusätzlich sollte das Praxispersonal in regelmäßigen Abständen für das Thema Diskretion sensibilisiert werden.

Bereits im Berichtszeitraum 2017/2018 haben wir das Thema der Diskretion in unserem Tätigkeitsbericht aufgegriffen: https://www.lda.bayern.de/media/baylda_report_08.pdf. Anhand der uns vorliegenden Beschwerden ist weiterhin Verbesserungsbedarf zu erkennen.

Hilfestellungen zur Umsetzung der Diskretion bietet u. a. die Broschüre der Kassenärztlichen Vereinigung Bayerns (KVB) „Datenschutz in der Arzt-/Psychotherapeutenpraxis“ (https://www.kvb.de/fileadmin/kvb/V10/Mitglieder/Service/Informationsservice/Informationsmaterial/Praxisbetrieb/KVB-Broschuere-Datenschutz-in-der-Praxis.pdf)

12.2 Patientenunterlagen zur Abholung als Aushang vor der Praxistüre

Durch den Aushang bzw. das Auslegen von Patientenunterlagen vor der Praxistür verstießen Ärzte gegen deren Pflichten dem Schutzniveau entsprechend angemessene technische und organisatorische Maßnahmen gemäß Art. 24 und 32 DS-GVO vorzuhalten.

Mehrere Beschwerden wurden bei uns eingereicht laut denen verschiedene Arztpraxen Arbeitsunfähigkeitsbescheinigungen bzw. Rezepte zur Abholung durch deren Patient:innen an der Außenseite der Praxistüre angebracht hatten bzw. auf einem Tisch vor der Praxistüre auslegten. Teilweise wurde dies auch um weitere Patientenunterlagen zur Abholung wie

Überweisungen oder Krankenkarten zum Einlesen erweitert. Durch dieses Vorgehen waren die vor dem Praxiseingang ausgehangenen bzw. ausgelegten Patientenunterlagen für unbefugte Dritte frei zugänglich.

Verantwortliche, worunter auch Leistungserbringer im Gesundheitsbereich zu fassen sind, haben gemäß Art. 24 und 32 DS-GVO angemessene technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Unter Beachtung des Selbstbestimmungsrechts der betroffenen Person und der Rechte weiterer betroffener Personen kann es in zu dokumentierenden Einzelfällen möglich sein, dass der Verantwortliche auf ausdrücklichen Wunsch der informierten betroffenen Person bestimmte vorzuhaltende technische und organisatorische Maßnahmen ihr gegenüber in vertretbarem Umfang nicht anwendet. Hierfür ist erforderlich, dass die betreffenden Patient:innen von der Praxis über das entstehende Risiko informiert wurden, dass z. B. unbefugte Dritte darauf Zugriff nehmen können, bevor die Unterlagen vor der Praxistüre angebracht bzw. ausgelegt wurden. Insbesondere wenn das Vorgehen telefonisch besprochen wurde, ist nicht per se davon auszugehen, dass die Patient:innen die Örtlichkeiten entsprechend kennen und sie über das entstehende Risiko bereits informiert sind.

13

Videoüberwachung

13 Videoüberwachung

13.1 Falschparker-Entscheidungen des VG Ansbach sind kein Freibrief für „Falschparker-Fotografen“

Wer Fotos in der Öffentlichkeit macht, um diese an Dritte weiterzuleiten, ist dem Datenschutzrecht unterworfen

Das Bayerische Verwaltungsgericht Ansbach hatte mit Entscheidungen vom 02.11.2022 zwei Verwarnungen gem. Art. 58 Abs. 2 Buchst. b DS-GVO zu „Falschparker-Fotografen“ von uns aufgehoben (Urteile vom 02.11.2022 - AN 14 K 22.00468 (https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-40163?hl=true) und AN 14 K 21.01431 (https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2022-N-38301?hl=true).

In beiden Verfahren wurden durch die Kläger verkehrswidrig parkende Kfz fotografiert, um den Verkehrsverstoß bei den zuständigen Ordnungsbehörden, insbesondere der Polizei, zur Anzeige zu bringen. Wir konnten mangels eigener Betroffenheit der Anzeigeerstatter jeweils keine Rechtsgrundlage zur Anfertigung von Fotografien und zur Übermittlung derselben an die Ordnungsbehörden erkennen. Insbesondere befanden wir Art. 6 Abs. 1 Buchst. f DS-GVO (Interessensabwägung) nicht als einschlägig, da wir insbesondere in Abgrenzung zu der Rechtsgrundlage des Art. 6 Abs. 1 Buchst. e DS-GVO (Wahrnehmung einer öffentlichen Aufgabe/ Ausübung öffentlicher Gewalt) ein berechtigtes Interesse sowie eine Erforderlichkeit an der (zusätzlichen zu der Anzeige an sich) Versendung des Bildmaterials mangels eigener Betroffenheit nicht sahen. Aus diesem Grund hatten wir einen Verstoß gegen den Grundsatz der Rechtmäßigkeit festgestellt.

Auch wenn unsere Verwarnungen von dem Gericht aufgehoben wurden, sehen wir uns im Grundansatz bestätigt. So äußert sich das Gericht dahingehend, dass das Vorgehen der „Fotografen“ im Anwendungsbereich der DS-GVO stattfindet und nicht als ein rein privater Vorgang im Sinne der Haushaltsausnahme gem. Art. 2 Abs. 2 Buchst. c DS-GVO anzusehen ist. Auch die Privatperson, die Fotografien von verkehrswidrig parkenden Kfz anfertigt, um diese an die zuständigen Ordnungsbehörden weiterzuleiten, ist somit in vollem Umgang der Geltung der DS-GVO unterstellt. Somit bleiben die Anzeigeerstattenden bei der Anfertigung und Weiterverarbeitung von Bildaufnahmen in der Pflicht, den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 Buchst. c DS-GVO zu beachten. Dies wird explizit durch das Gericht hervorgehoben und bedeutet, dass insbesondere keine personenbezogenen Daten anderer Personen oder Kfz-Kennzeichen unbeteiligter Fahrzeuge übermittelt werden dürfen. Weiterhin sind den grundlegenden Betroffenenansprüchen wie dem Recht auf Auskunft oder Löschung nachzukommen und auch die Einbindung weiterer Akteure bedarf einer datenschutzrechtlichen Grundlage.

Die rechtskräftigen Entscheidungen des Gerichts stellen somit keinen Freibrief für „Falschparker-Fotografen“ dar (vgl. hierzu auch unsere Pressemitteilung vom 2. Januar 2023 unter https://www.lda.bayern.de/media/pm/pm2023_01.pdf).

13.2 Videoüberwachung in Fitnessstudios

Videoüberwachung von Trainingsflächen in Fitnessstudios ist unzulässig

Wir untersagten im Berichtszeitraum in Folge einer Beschwerde die Beobachtung der Trainings-

flächen in einem Fitnessstudio während Öffnungszeiten mittels optisch-elektronischer Einrichtungen (Videoüberwachung) und die Anfertigung von Bildaufzeichnungen.

Für die Überwachung der Trainingsflächen mittels Videokameras und die Anfertigung von Bildaufzeichnungen konnten wir keine Rechtsgrundlage erkennen. Weder konnte der Argumentation des Fitnessstudiobetreibers gefolgt werden, dass mit dem Betreten des Fitnessstudios trotz Auszeichnung der Videoüberwachung eine wirksame Einwilligung, die den Anforderungen der Art. 4 Nr. 11, 7 DS-GVO gerecht wurde, in die Videoüberwachung abgegeben wurde. Auch konnte die Videoüberwachung nicht auf Art. 6 Abs. 1 Buchst. b DS-GVO gestützt werden, da kein Zusammenhang einer Notwendigkeit der Videoüberwachung mit dem Zweck des Vertragsverhältnisses bestand. Ebenso lagen die Voraussetzungen des Art. 6 Abs. 1 Buchst. f DS-GVO nicht vor. Zwar brachte der Fitnessstudiobetreiber vor, dass mit der Videoüberwachung u.a. Diebstähle, Sachbeschädigungen verhindert bzw. verfolgt werden sollten, jedoch konnte insbesondere keine Erforderlichkeit für die ganzheitliche Videoüberwachung nachgewiesen werden. Wir sahen die Interessen der betroffenen Personen hier als die berechtigten Interessen des Verantwortlichen überwiegend an.

Gegen diese Untersagungsverfügung ging der Fitnessstudiobetreiber vor und legte Klage beim Bayerischen Verwaltungsgericht Ansbach ein. Dieses bestätigte in erster Instanz unsere Untersagungsverfügung (VG Ansbach, Urteil v. 23.02.2022 – AN 14 K 20.00083). Auch das Gericht sah in der bloßen Kenntnisnahme des Hinweisschildes keine eindeutige bestätigende Handlung der Trainierenden. Eine Erforderlichkeit für die Vertragserfüllung gem. Art. 6 Abs. 1 Buchst. b DS-GVO wurde nicht bejaht, da eine lückenlose Videoüberwachung über die Pflichten, die aus vertraglichen Nebenpflichten wie Rücksichtnahme- und Schutzpflichten (z.B. Schutz vor Übergriffen und Diebstählen) bestehen können, hinausging. Hinsichtlich des Art. 6 Abs. 1 Buchst. f DS-GVO führte das Gericht aus, dass sowohl zwar berechtigte Interessen gegeben sind - zum einen eigene Interessen des Verantwortlichen (Prävention und Verfolgung von Diebstahl und Sachbeschädigung) und zum anderen Interessen der Trainierenden (Schutz vor Diebstahl und Übergriffen). Allerdings überwiegen aus Sicht des Gerichts die Interessen der Trainierenden ohne Beobachtung zu trainieren, da es sich um einen gravierenden Eingriff ohne räumliche und zeitliche Ausweichmöglichkeit handelt. Alleine der Umstand, dass die Videoüberwachung gegenüber einer Personalaufstockung die wirtschaftlich sinnvollere Alternative sei, reiche ebenfalls nicht aus, um eine andere Interessengewichtung zu erreichen. Zudem sei bei der Interessenabwägung zu berücksichtigen, dass gemäß Satz 4 des DS-GVO-Erwägungsgrundes 47 insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen können. Unter Bezugnahme auf die Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte (Version 2.0) schloss sich das Gericht dem Grundsatz an, dass betroffene Personen davon ausgehen dürfen, dass sie nicht überwacht werden, insbesondere wenn diese Bereiche typischerweise für Freizeitaktivitäten genutzt werden, wie es bei Fitnesseinrichtungen der Fall ist. Auch die vom Fitnessbetreiber dargestellten Schäden führten nach Ansicht des Gerichts nicht dazu, dass in dem konkreten Verfahren eine andere Interessensgewichtung als geboten betrachtet wurde. Im Urteil selbst wurde zudem deutlich gemacht, dass die Risiken der Aufklärbarkeit von Diebstählen oder Übergriffen, primär im Verantwortungsbereich der Trainierenden selbst läge und diese das Risiko beispielsweise durch Einsperren von Wertgegenständen, Wahl von Trainingsgeräten in

der Nähe der Empfangstheke bzw. Trainieren zu „risikoärmeren" Uhrzeiten selbst senken könnten.

Das Urteil des Bayerischen Verwaltungsgerichts Ansbach ist noch nicht rechtskräftig. Der Kläger hat Berufung eingelegt.

13.3 Videoüberwachung in der Gastronomie

Videoüberwachung von Bewirtungsflächen ist in der Regel unzulässig

Immer wieder erreichen uns Beschwerden bezüglich einer Videoüberwachung in der Gastronomie. Beschwerdegegenstand ist dabei häufig die Überwachung, d.h. Beobachtung und ggf. auch Aufzeichnung mittels optisch-elektronischer Einrichtung, von Gasträumen oder von Außenflächen, die bewirtschaftet werden. Von dieser Überwachung betroffen sind in der Regel sowohl die Gäste als auch das Personal.

Eine Rechtsgrundlage für die Videoüberwachung von Gästen ist in der Regel nicht gegeben. Auch wenn auf die Videoüberwachung mittels Hinweisschildes hingewiesen wird, kann selbst bei Lesen dieses Hinweisschildes dies nicht als Einwilligung in die Datenverarbeitung (vgl. Art. 6 Abs. 1 Buchst. a DS-GVO) gelten, da die Anforderungen an eine ausdrückliche Einwilligung in die Datenverarbeitung gem. Art. 4 Nr. 11, 7 DS-GVO nicht erfüllt sind. Auch ist die Videoüberwachung der Bewirtungsflächen nicht von der Rechtsgrundlage Art. 6 Abs. 1 Buchst. f DS-GVO (Interessenabwägung) gedeckt. Häufig können zwar berechtigte Interessen erkannt werden, allerdings kann die Erforderlichkeit häufig nicht begründet werden und führt die Interessenabwägung zu dem Ergebnis, dass die Interessen der betroffenen Personen überwiegen. Im Regelfall kann eine besondere Gefährdungslage für das Eigentum oder die körperliche Unversehrtheit nicht dargelegt werden. Bei der Interessenabwägung sind gemäß Erwägungsgrund 47 die vernünftigen Erwartungen der betroffenen Person zu berücksichtigen. Gäste eines Gastronomiebetriebes können davon ausgehen, dass sie in öffentlich zugänglichen Bereichen nicht überwacht werden, vor allem, wenn diese Bereiche typischerweise für Erholungs-, Entspannungs- und Freizeitaktivitäten genutzt werden, sowie an Orten, an denen sich Personen aufhalten und/oder kommunizieren, wie z. B. Sitzbereiche, Tische in Restaurants (vgl. EDSA-Leitlinien3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rn. 28).

Bezüglich des von der Überwachung der Bewirtungsfläche mit erfasstem Personal kommt es zudem darauf an inwieweit die Mitarbeiterdaten zu Zwecken einer Leistungs- und Verhaltenskontrolle verarbeitet werden sollen. Die Verarbeitung der Beschäftigtendaten zu diesem Zweck richtet sich nach Art. 6 Abs. 1 Buchst. b DS-GVO[4].

Die Überwachung öffentlicher Verkehrsflächen, wie z.B. an Außenflächen angrenzende Fußwege sowie Straßen ist grundsätzlich unzulässig.

[4] Im Lichte der EuGH-Rechtsprechung in der Rechtssache C-34/21 sehen wir § 26 Abs. 1 S. 1 BDSG nicht für anwendbar an.

14

Cybersicherheitslage

14 Cybersicherheitslage

Die Anzahl von Datenschutzverletzungen aufgrund komplexer Cyberattacken bleibt auf hohem Niveau. Für die gründliche Bearbeitung der Vorfälle ist trotz Priorisierung weiterhin zu wenig Personal vorhanden.

14.1 Gefährdungslage

Im Jahr 2022 dominierte wie in den Vorjahren schon die Bearbeitung von Meldungen nach Art. 33 die Arbeit des technischen Bereichs „Cybersicherheit und technischer Datenschutz". Eine Meldung bei der Aufsichtsbehörde ist erforderlich, wenn Verantwortliche eine Verletzung der Sicherheit bei der Verarbeitung personenbezogener Daten feststellen und mindestens ein Risiko der Rechte und Freiheiten für die betroffenen Personen vorhanden ist. Der wirtschaftsstarke Standort Bayern mit Unternehmen aus allen Bereichen der Wertschöpfungskette stellt damit zwangsläufig ein attraktives Angriffsziel für cyberkriminelle Gruppierungen dar, da vernetzte Datenflüsse und ein hoher Digitalisierungsgrad vielfältige Angriffsmöglichkeiten mit sich bringen. In der Gesamtschau der eingegangenen Meldungen können diese in drei Hauptkategorien unterteilt werden:

1. Cyberangriffe von kriminellen Gruppierungen

Weiterhin binden sogenannte Ransomware-Angriffe weiterhin große Bearbeitungsressourcen der Behörde. Die Angreifergruppierungen, die regelmäßig auf einem professionellen Niveau arbeiten, gelangten meist über fehlerhafte Softwarestände bei über das Internet erreichbaren Netzwerkkomponenten (z.B. Firewalls oder VPN-Appliances) oder über Social Engineering Angriffe (meist mittels E-Mail-Anhängen oder in E-Mails eingebetteten Links) auf ein IT-System bei den Unternehmen. Auf Grund ihrer Fortbewegungsmöglichkeiten im Netzwerk wurden dann – fast wie aus dem „Lehrbuch" - (lokale) Adminstratorrechte erlangt und nicht selten auch zentrale Einheiten wie den Domain Controller (unter Windows Systemen) unter Kontrolle gebracht. Auch Linux-Systeme, insbesondere als sogenannte Hosts von virtuellen Maschinen, waren beliebte Angriffsziele, da so der Angriffsschaden maximiert werden kann. Vor einer Verschlüsselung der (personenbezogenen) Daten fand fast immer eine Datenausleitung auf Server im Internet statt – das als „Double Extorsion" benannte Vorgehen stellte im Jahr 2022 den Standard bei Ransomware-Angriffen auf Unternehmen dar. Nach der Ausleitung der Daten fand in den meisten gemeldeten Fällen eine (aus Sicht der Angreifer) erfolgreiche Verschlüsselung der Daten statt, häufig nachdem die Backups entweder gelöscht oder (teilweise) auch verschlüsselt wurden. Lösegeldforderungen in Millionenhöhe waren in dem Großteil der Fälle Standard, wobei sich die Zahlungsbereitschaft der Unternehmen meist davon abhingen inwieweit sie den operativen Betrieb aus eigener Kraft wieder aufzunehmen vermochten.

Angriffe von staatlicher Seite (auch im Kontext des Ukraine-Kriegs) waren in 2022 aus datenschutzrechtlicher Perspektive nicht bewertbar, da hierzu keine belegbaren Informationen vorlagen.

Sogenannte Supply-Chain-Angriffe (Angriffe auf Dienstleister oder Softwareprodukte, die bei vielen Unternehmen zum Einsatz kommen) wurden teilweise festgestellt und konnten meist bekannten cyberkriminellen Gruppierungen zugeordnet werden. Aufgrund der regelmäßig hohen Zahl betroffener Unternehmen stellen Supply-

Chain-Angriffe zunehmend eines der größten Risiken für bayerische Unternehmen dar.

Neben den Ransomwareangriffen haben wir eine Zunahme der Meldungen von erfolgreichen Angriffen auf Cloud-Systeme festgestellt. Insbesondere die Cloud-Anwendung Microsoft 365 dominierte das Meldegeschehen, wobei dabei fast ausschließlich Angriffe über die Entwendung von Zugangsdaten mittels Social Engineering (z.B. E-Mail mit Link auf gefälschte Microsoft365 Login-Seite) erfolgten. Waren den Angreifern (nicht selten mit Administratorrechten) Microsoft 365 Konten zugänglich, wurden häufig E-Mail-Weiterleitungen eingerichtet oder das Konto für den Versand von Schadcode-Mails missbraucht. Die Feststellung, ob Dokumente (z.B. bei Einsatz von OneDrive) ebenfalls entwendet wurden, war häufig mangels Protokollierung nicht möglich.

Meldungen zu dezidierten Schadcodevorfällen haben sich auf einen mittleren einstelligen Zahlen-Niveau eingependelt, wobei diese eher ein Anhaltspunkt für eine gut funktionierenden Datenschutzorganisation beim meldenden Unternehmen denn für eine Aussage zu quantitativen Gegebenheiten sein dürften.

2. Softwarefehler und Fehlkonfigurationen

Sicherheitsverletzungen, die keine kriminelle Ursache haben, sondern durch einen nicht sachgemäßen IT-Betrieb verursacht werden, traten auch 2022 nurmehr in durchschnittlicher Höhe auf. Bei diesen werden bspw. Firewalls nicht korrekt konfiguriert, so dass Unbefugte ohne Überwindung von Zugangssicherungen auf interne IT-Systeme zugreifen können oder versehentlich veröffentlichte Passwörter von Datenbanken, die entgegen den Vorgaben des Art. 32 DS-GVO ohne Schutz einer Firewall ebenfalls direkt aus dem Internet erreichbar sind, zu einem Komplettzugang bspw. von personenbezogenen Daten eines Online-Shops führen. Wir haben von derartigen Fällen neben der Meldung von Unternehmen, die diese Fehlkonfigurationen selbst festgestellt hatten, auch über Hinweise von IT-Sicherheitsforschenden oder durch Datenschutzbeschwerden Kenntnis erlangt und alle unbefugten Zugriffsmöglichkeiten durch aufsichtliche Maßnahmen innerhalb eines Arbeitstages abstellen können.

3. Informationsweitergabe und Fehlversendungen

Auch Verletzungen der Vertraulichkeit von nichtdigitalen personenbeziehbaren Informationen unterliegen ebenfalls der Meldepflicht des Art. 33 DS-GVO. Dies sind bspw. postalische Fehlversendungen. Im Berichtszeitraum waren insoweit keine nennenswerten Besonderheiten festzustellen.

14.2 Detailbetrachtung

Im Berichtszeitraum ist die Anzahl der Meldungen nach Art. 33 DS-GVO auf 2991 zurückgegangen. Ein genauerer Blick zeigt allerdings keine Abnahme der grundsätzlichen Gefährdungslage, sondern eine Verschiebung hin zu komplexeren Angriffen mit einer zeitgleichen deutlichen Abnahme der Meldungen im Bereich bloßer Fehlversendungen. Im Einzelnen zeigen sich folgende Entwicklungen:

1. Ransomware

Mit 296 erfolgreichen Ransomwareangriffen bei bayerischen Unternehmen in 2022 hat sich das Niveau ungefähr auf den Zahlen des Vorjahres eingependelt. Eine Verschiebung der Angreifergruppierungen fand entsprechend der regelmäßigen Neuorganisationen der Gruppierungen statt (bspw. haben 2022 die Ransomware-Gruppierungen Blackbasta und Lockbit die meisten Meldungen verursacht).

2. Angriffe auf Cloud-Dienste

Mit 312 Meldungen haben die Angriffe auf Cloud-Dienste insbesondere mit dem Zweck einer missbräuchlichen Verwendung der damit verbundenen E-Mail-Infrastruktur weiterhin ein hohes und ernstzunehmendes Niveau erreicht. Die Quelle der Angriffe konnte in den meisten Fällen nicht festgestellt werden. Eine markante Entwicklung bleibt der Versand von Schadcode an viele Empfänger, mitunter auch außerhalb der üblichen Kommunikationsspähre des Unternehmens..

3.Supply-Chain-Angriffe

Die Fallzahlen von Supply-Chain-Angriffen wurden in 2022 noch nicht systematisch erfasst. Einzelfälle wie ein Dienstleister mit 130 Meldungen zu betroffenen Unternehmen in Bayern zeigen aber jetzt schon das Risikopotential derartiger Angriffsarten.

4. Diebstahl-/und Verlustmeldungen

Fallzahlen insbesondere bei nichtverschlüsselten Datenträgern im niedrigen dreistelligen Bereich zeigen, dass derartige Vorfälle, so gravierend diese im Einzelfall sein können (z.B. bei Gesundheitsdaten oder Personalratsunterlagen) in der Betrachtung der Anzahl aller bayerischer Unternehmen verschwindend gering sind, auch wenn eine erhöhte Dunkelziffer nicht auszuschließen ist.

5. Fehlkonfigurationen

Eine niedrige dreistellige Anzahl von Meldungen zu Fehlkonfigurationen weist auf Sachverhalte hin, die bspw. in polizeilichen Statistiken aufgrund des Mangels eines kriminellen Hintergrunds meist gar nicht auftauchen. Da zudemhäufig eine unzureichende Protokollierung der IT-Systeme keine Datenabflüsse aufzuzeigen vermag, ist bislang die Bewertung von Risikohöhen für die Verantwortlichen eine enorme Herausforderung. Im Zweifel ist regel-mäßig auf Grund einer Zwei Worst-Case-Betrachtungeine Information der Betroffenen nach Art. 34 DS-GVO geboten, da dann von einer maximalen Eintrittswahrscheinlichkeit ausgegangen wird.

14.3 Fallbeispiele

Im Im Folgenden werden einige exemplarische Fälle kurz und ohne Nennung des Unternehmensnamen dargestellt.

1. Ein DAX-Unternehmen im Bereich Mobilität wurde im Frühjahr 2022 Opfer der Gruppierung BlackBasta, die seit Frühjahr 2022 zunehmend durch spektakuläre Cyberangriffe auf sich Aufmerksam gemacht hat. Aufgrund der neuartigen Gruppierung und der hohen Komplexität des Angriffs haben wir eine umfangreiche Datenschutzkontrolle durchgeführt.

2. Ein Unternehmen aus der Baustoff-Branche wurde Im Juni 2022 ebenfalls Opfer der Gruppierung BlackBasta. Auch hier zeigte sich ein hochprofessionelles Vorgehen der Angreifer,

4. Die Gruppierung Royal hat im Oktober ein Unternehmen aus dem Bereich Tourismus erfolgreich angegriffen. Die mehr als 100.000 betroffenen Endkund:innen hatten dabei wohl Glück im Unglück: Die Befürchtung eines Datenabflusses wurde in Rahmen der Aufarbeitung mit hoher Wahrscheinlichkeit nicht bestätigt.

5. Die Gruppierung Hive hat im Frühsommer bei einem bayerischen IT-Dienstleister einen erfolgreichen Angriff mit Verschlüsselung und Datenausleitung durchgeführt. Dieser Angriff führte zu einer Reihe von Folgemeldungen durch Verantwortliche (alleine 40 im nicht-öffentlichen Bereich Bayern), die diesen Dienstleister im Rahmen einer Auftragsverarbeitung eingesetzt hatten. Derartige Supply-Chain-Angriffe sind durch die bereits bestehenden gesetzlichen Regelungen der DS-GVO zur Meldepflicht bei der Datenschutzaufsichts-behörde gut abgedeckt.

6. Eine missliche Entdeckung hat ein bayerisches StartUp bei einem Blick auf deren Webseiten-HTML Quelltext gemacht: Der Admin-Accesstoken war dort fälschlicherweise ersichtlich, mit dem ein Angreifer Zugang zu den Kundendaten hätte erlangen können. Da im Rahmen der Aufarbeitung ein derartiger Zugriff mit hoher Wahrscheinlichkeit ausgeschlossen werden konnte, war die Voraussetzung einer Meldung bei den betroffenen Personen nach Art. 34 DS-GVO nicht erfüllt.

7. Ein Kunde einer Online-Apotheke hat seine beruflichen Fertigkeiten im Bereich IT-Sicherheit angewendet, als sein Registrierungsversuch auf einer neu gestarteten Webpräsenz fehlschlug, die Fehlermeldungen aber Hinweise auf authentifizierte Datenabrufmöglichkeiten offenbarte. Nachdem dieser Rezepte und Kopien mehrerer Versicherungsausweise ohne Überwindung einer Zugangssicherung abrufen konnte, wurden wir im Rahmen einer Beschwerde über den Sachverhalt informiert. Die Compliance-Prozesse der Apotheke haben im Nachgang gut funktioniert: Die Lücke wurde geschlossen und eine Auswertung der Log-Dateien ergab mit hoher Wahrscheinlichkeit keinen missbräuchlichen Zugriff auf die nicht angemessen gesicherten Kundendaten.

8. Eine Möglichkeit des Zugriffs auf den kompletten Kundenstamm mit mehr als 150.000 betroffenen Personen eröffnete ein Online-Shop im Bereich Lebensmittel, nachdem die Zugangsdaten der Datenbank über eine unzu-reichende Sicherung einer Anwendung zur internen Softwareentwicklung über das Internet aufrufbar waren. Neben einer mangelhaften Konfiguration der Firewall stellte sich auch die Frage, wieso Datenbank-Passwörter im Klartext auf internen Webanwendungen ge-speichert werden mussten – eine überzeugen-de Antwort konnte wenig überraschend nicht geliefert werden. werden.

14.4 Cyberabwehr Bayern

Die im letzten Tätigkeitsbericht bereits vorgestellte Cyberabwehr Bayern, eine Kooperationsplattform bayerischer Behörden mit Cybersicherheitsaufgaben, spielte auch im Berichtszeitraum für den technischen Datenschutz eine wichtige Rolle bei der Bearbeitung schwerer Cybersicherheitsvorfälle. Wir schätzen die mittlerweile bestens etablierten wöchentlichen Lagebesprechungen als wichtigen Baustein der gemeinsamen Bemühung aller bayerischen Sicherheitsbehörden mit Cybersicherheitsaufgaben ein, Cybersicherheitsvorfälle schnell aufzuklären und Informationen im Rahmen der gesetzlichen Möglichkeiten zu Bedrohungslagen und Angreifervorgehen zu teilen. Das BayLDA ist ein bedeutenderer Anker der Cyberabwehr Bayern insbesondere zu Vorfällen aus dem Bereich der kleineren und mittelständischen bayerischen Wirtschaft (KMU) und hat aufgrund der vielen Meldungen nach Art. 33 DS-GVO eine äußerst aktuelle und mit Blick auf z.B. Angriffsvektoren auch detaillierte Vorstellung davon, wie kriminelle Cyber-Gruppierungen in Bayern agieren. Wir sind der Auffassung, dass die in den wöchentlichen Lagesitzungen erarbeiteten Erkenntnisse in einem zukünftig möglicherweise umfassenderen Tätigwerden der Cyberabwehr Bayern auch in Präventionsangebote insbesondere für KMUs und kleinere medizinische Einrichtungen verwendet werden könnten, um das "bayerische Abwehrschild" auch über diese mit aufzuspannen. Wir würden in diesem Fall dann gerne unseren Beitrag für diese Aufgabe leisten– entsprechende personelle Ressourcen natürlich vorausgesetzt.

14.5 Bewertung und Prognose

Mit Blick auf die in 2022 in einer Gesamtschau zwar abnehmende Anzahl von Art. 33 Meldungen, die aber keinen nennenswerten Rückgang bei schwere Cyberattacken beinhalten, führt zu

unserer Einschätzung, dass in den meisten erfolgreich durchgeführten Cyberangriffen auch ein Verstoß gegen technische und organisatorische Maßnahmen nach Art. 32 DS-GVO im Vorfeld vorlag, der den Angriff erst ermöglichte. Im Einzelfall durchgeführte intensivere Detailkontrollen (auch mit Vor-Ort-Besuchen) haben dabei fast durchgängig ein Bild ergeben, dass IT-Sicherheit bei den Unternehmen zwar grundsätzlich einen hohen Stellenwert einnimmt, die Vielzahl von teils hochpreisigen Security-Produkten alleine allerdings einen erfolgreichen Cyberangriff nicht verhindern konnten. Für uns stellt sich bei dem „Katz und Maus Spiel" zwischen Angreifern und Verteidigern die Frage, wie eine Abwehr von Cyberangriffen bei den bayerischen Unternehmen noch zuverlässiger gelingen könnte.

Nach unserer Auffassung müssten zumindest die Ansätze „Defense-In-Depth" und „Zero Trust", bei dem hauptsächlich nicht nur der (Netzwerk-)Perimeter durch Firewalls, IOCs-Sperrlisten und Malware-Schutz geschützt ist, umfassender beachtet werden. Dabei sollte immer eine zentrale Frage im Raum stehen: Welche Möglichkeiten hat ein:e fachlich sehr qualifizierte:r Angreifer:in, der/die einen einzelnen Rechner innerhalb des Unternehmensnetzes unter seine/ihre Kontrolle gebracht hat und dezidierte Angriffstools wie bspw. Cobalt Strike einsetzt? Gerade der Teil einer Angriffskette, bei dem ein:e Angreifer:in, sich bereits innerhalb des Unternehmensnetzes befindet (bspw. nachdem ein Schadcode durch Click auf ein per Mail zugesandtes Dokument aktiviert wurde), sich so Zugang zu Zentralservern oder Dateiablagen verschafft und dabei zudem administrative Rechte erlangt (nennt sich „Lateral Movement" und „Privilege Escalation") konnte nur in einem kleinen Teil der Ransomwareangriffe in der nachfolgenden Aufarbeitung plausibel aufgeklärt werden.

Sollte ein:e Angreifer:in personenbezogene Daten entwenden und/oder verschlüsseln, ist der Schaden meist irreversibel. Dabei spielt es aus datenschutzrechtlicher Sicht keine Rolle, ob ein Lösegeld gezahlt wird oder nicht, da wir bei kriminellen Gruppierungen immer von der maximalen missbräuchlichen Verwendung personenbezogener Daten ausgehen müssen. Zusicherungen von manchen kriminellen Gruppierungen, nach einer Lösegeldzahlung die entwendeten (personenbezogen) zu löschen, kann mangels „Treu und Glauben" nach Art. 5 Abs. 1 DS-GVO kein Glauben geschenkt werden– die „Ehre unter Dieben" ist im Datenschutzrecht aus gutem Grund nicht verankert.

Da den Grenzen der repressiven Strafverfolgung im Bereich Cybercrime Grenzen gesetzt sind, da Angreifer meist unerkannt aus dem außereuropäischen Ausland agieren, kommt der Cyberprävention durch Verantwortliche nach DS-GVO zur Sicherstellung eines angemessenen Schutzniveaus nach Art. 32 DS-GVO eine besondere Bedeutung zu. Aus diesem Grund haben wir in 2022 einen Schwerpunkt auf Datenschutzkontrollen mit dem Fokus „Ransomware-Prävention" und „E-Mail Account Absicherung" gesetzt. Die dabei versendeten Prüfbögen samt einer Handreichung für technische und organisatorische Maßnahmen zum Schutz für Cyberangriffen sind auf unserer Webseite unter „Startseite->Datenschutzprüfungen" abrufbar. Darin sind Schutzmaßnahmen beschrieben, durch deren Umsetzung unserer Meinung nach ein bedeutender Teil der in 2022 erfolgreichen Cyberangriffe hätte verhindert werden können– qualitätsgesichert wird diese Behauptung durch unsere Aufarbeitung von Art. 33 Meldungen mit Blick auf die bislang erfolgreichen Angriffsgeschehen. Die betrieblichen Datenschutzbeauftragten sollten diesbezüglich ermutigt werden, diese Checklisten in die eigenen Datenschutzkontrollen mit einzubauen. Denn eines eint Wirtschaftsunternehmen und Datenschutzauf-

sichtsbehörden: Eine wirksame Abwehr von Cyberangriffen ist im Interesse der Grundrechte und Grundfreiheiten sowohl der Bürgerinnen und Bürger als auch der bayerischen datenschutzrechtlichen Verantwortlichen.

Mangels Ressourcen können aktuell leider keine Beratungen für Verantwortliche zur Umsetzung von Präventionsmaßnahmen zum Schutz vor Cyberangriffen durch unsere Behörde angeboten werden können. Zeitgleich muss eine wirksame und effektive Datenschutzaufsicht gewährleistet werden.
Während die durchgeführten Datenschutzkontrollen in 2022 noch einen sensibilisierenden Charakter hatten, werden zukünftig zunehmend Sanktionen in Form von Geldbußen und Anordnungen zu Abhilfemaßnahmen zu prüfen sein, sollten Verstöße gegen Art. 32 DS-GVO im Rahmen einer Kontrolle festgestellt werden.

Verstöße gegen Cybersicherheitsmaßnahmen können gem. Artikel 83 Abs. 4 Buchstabe a) DSGVO mit bis zu 2% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres sanktioniert werden - ironischerweise in der selben Größenordnung, in der sich Ransomware-Gruppierungen mit ihren Lösegeldforderungen bewegen.

15

Datenschutzkontrollen

15 Datenschutzkontrollen

15.1 Ransomware-Präventionsprüfung als Dauerprüfung

Die Ende 2021 gestartete Ransomware-Präventionsprüfung wurde aufgrund der hohen Bedrohungslage als Dauerprüfung etabliert

Wie im letzten Tätigkeitsbericht bereits dargelegt, hat die im Herbst 2021 neu gegründete Stabstelle Prüfverfahren des LDA mit einer Ransomware-Präventionsprüfung den Startschuss für eine Reihe anlassloser fokussierter Kontrollen gegeben. Aufgrund der guten Erfahrungen mit dieser Prüfreihe bei 30 bayerischen Verantwortlichen und der Einschätzung, dass nach wie vor bayerische Verantwortliche von den in der Prüfung bereitgestellten Checklisten im Kontext Cyberprävention profitieren könnten, haben wir uns im Herbst 2022 entschieden, die Ransomwareprüfung bis zum Abklingen dieser Art der Cyberbedrohung in Bayern als Dauerprüfung zu etablieren. Im Detail wurden die Kernbereiche

- Systemlandschaft
- Patch Management
- Backup-Konzept
- Überprüfung des Datenverkehrs
- Awareness und Berechtigungen

abgefragt, mit denen ein bedeutender Umfang der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO zur Sicherstellung eines angemessenen Sicherheitsniveau gegen Ransomware-Bedrohungen erreicht werden kann .

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

15.2 Kontrolle E-Mail-Sicherheit

Aufgrund der spürbaren Steigerung der Bedrohungslage für Cyberangriffe auf Email-Dienste haben wir eine neue Prüfreihe für (bei Dienstleistern) betriebene Email-Accounts gestartet

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

Da wir seit Ende 2021 ein verstärktes Aufkommen von Cyberattacken auf E-Mail-Accounts von Verantwortlichen in Bayern registriert haben, bei dem oft das Abgreifen der enthaltenen vertraulichen E-Mail-Kommunikation im Vordergrund, um bspw. Finanztransaktionen zu manipulieren, stand, haben wir uns für eine Kontrolle bei (erst einmal) 98 bayerischen Verantwortlichen in diesem Themenbereich entschieden.

Durch einen erfolgreichen Angriff auf einen Email-Account können auch nachgelagerte Angriffe, die ein tieferes Eindringen in die Netzwerkstruktur ermöglichen oder die für die Weiterverbreitung von Schadsoftware auf die Systeme der Kontakte (z. B. Kunden) sorgen, stattfinden. Bereits nach der Kompromittierung eines einzelnen E-Mail-Accounts werden von den Cyberkriminellen meist alle Kontakte mit gefälschten E-Mails angeschrieben. Die eigentlichen Ursachen solcher Cyberangriffe sind nicht selten in einer unsachgemäßen Bedienung (u. a. auf Grund mangelndem Sicherheitsbewusstsein bei den Beschäftigten) oder in einer fehlerhaften Konfiguration und Absicherung der E-Mail-Accounts zu finden. Durch Homeoffice haben

sich zudem in einigen Betrieben die diesbezüglich ohnehin schon bestehenden Sicherheitsgefährdungen weiter verschärft, da dies meist mit einer umfassenderen Verwendung von Cloud-Diensten einherging.

15.3 Fokussierte Prüfung Selbstauskünfte Mietinteressentinnen

Selbstauskunftsbögen für Mietinteressentinnen müssen sich insbesondere am Grundsatz der Erforderlichkeit messen lassen

Trotzdem sich die deutschen Aufsichtsbehörden mittels einer Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen (Link unten) positioniert haben, stellten wir bei der Beschwerdebearbeitung im Bereich Wohnungswirtschaft immer wieder fest, dass gerade in Ballungsgebieten Mietinteressent:innen bereits im Rahmen einer Erstbesichtigung einer Wohnung ein umfangreiches Formular zur Selbstauskunft zur Verfügung gestellt wurde. Dieses sollte meist im Vorfeld ausgefüllt werden und entweder bereits vor oder spätestens zum Erstbesichtigungstermin, oftmals jedenfalls aber bei Gefallen der besichtigten Wohnung dem/der Eigentümer:in bzw. dem/der beauftragten Immobilienmakler:in übergeben werden.

Aus diesem Grund entschlossen wir uns, eine anlasslose und fokussierte Prüfung zu diesem Themenbereich durchzuführen. Grundlage für den von uns verschickten Prüfungsbogen war die o.g. Orientierungshilfe, die die Zulässigkeit von Datenverarbeitung zu den unterschiedlichen Zeitpunkten darstellt. Die Prüfaktion wurde durch die Stabstelle Prüfverfahren koordiniert, so dass nach deren Konzeption sowohl der Prüfbogen an sich, aber auch das Anschreiben an die Prüflinge sowie weitere Informationen zur Verfügung gestellt wurden.

Im Rahmen der durchgeführten Prüfung wurden bei den geprüften Verantwortlichen keine Verstöße festgestellt, die mittels Maßnahmen gem. Art. 58 Abs. 2 DS-GVO geahndet wurden. Allerdings wurden einige Verantwortliche angehalten, ihre Selbstauskunftsbögen anzupassen.

Die Prüfungsunterlagen werden auch weiterhin in anlassbezogenen Prüfungen als Grundlage genutzt und können weiterhin auf unserer Homepage zur Orientierung und Information abgerufen werden.

Leider hat unsere Prüfung und die Veröffentlichung der Informationen jedoch nicht dazu geführt, dass alle Verantwortlichen in unserem Zuständigkeitsbereich ihre Selbstauskunftsbögen angepasst haben. Weiterhin erreichen uns zahlreiche Beschwerden bzw. stellen wir fest, dass die Vorgaben der DS-GVO insbesondere im Hinblick auf die Erforderlichkeit der Datenverarbeitungen nicht durchgehend eingehalten werden, so dass nunmehr weitere (Bußgeld-)Verfahren eingeleitet wurden.

https://www.datenschutzkonferenz-online.de/media/oh/20180207_oh_mietauskuenfte.pdf

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

16

Bußgeldverfahren

16 Bußgeldverfahren

16.1 Bericht aus der Zentralen Bußgeldstelle (ZBS)

Ein großer Teil der von der ZBS im Berichtszeitraum bearbeiteten Fälle betraf den Einsatz von GPS-Trackern, Dashcams und fest installierter Videoüberwachung durch Privatpersonen sowie die Veröffentlichung personenbezogener Informationen (wie etwa von Bildern oder Telefonnummern) im Internet, die aufgrund von Privatanzeigen von der Polizei an die ZBS übermittelt wurden.

Bei dem Einsatz von GPS-Trackern stellt sich regelmäßig die Frage, ob hierfür im konkreten Fall überhaupt der Anwendungsbereich der DS-GVO eröffnet ist, da die Verwendung in vielen Fällen unter die Haushaltsausnahme fällt, insbesondere wenn dieser GPS-Tracker zur Ortung von Familienangehörigen desselben Haushalts genutzt wird.

Eine allgemein zugängliche Bereitstellung im Internet ist dagegen nicht mehr von der Haushaltsausnahme gedeckt (vgl. Kapitel 4.1), so dass diese Veröffentlichung an den Kriterien der DS-GVO zu messen ist. In der Regel fehlt es für diese bereits an einer Rechtsgrundlage.

Der zulässige Einsatz von in Fahrzeugen installierten Kameras (sog. Dashcams) war bereits Gegenstand verschiedener Tätigkeitsberichte in der Vergangenheit (vgl. 7. Tätigkeitsbericht (Ziff. 19.6), 8. Tätigkeitsbericht 2017/2018 (Ziff. 19.1). In diesen wurde schon mehrfach darauf hingewiesen, dass eine permanente, anlasslose Aufzeichnung des Verkehrsgeschehens mit einer Videokamera datenschutzrechtlich unzulässig ist. Gleichwohl werden Dashcams oftmals noch immer nicht datenschutzkonform eingesetzt. Auch im Übrigen entspricht der Einsatz von Videoüberwachung vielfach noch immer nicht den Anforderungen der DS-GVO.

Nicht bei allen der Bußgeldstelle gemeldeten Verstößen wurde die Durchführung eines Bußgeldverfahrens eingeleitet bzw. ein bereits von der Polizei eingeleitetes Verfahren fortgeführt. Zur Gewährleistung der einheitlichen Anwendung der DS-GVO wurden vorrangig solche Fälle in ein Bußgeldverfahren überführt oder in einem solchen weiterbehandelt, bei denen aus den in der Verordnung angelegten spezial- und generalpräventiven Aspekten die Verhängung einer Geldbuße im Einzelfall für eine effektive Sanktionierung von Datenschutzverstößen geboten ist. Beispielhaft gilt dies etwa für den Fall heimlicher Videoaufnahmen an einem Badegewässer, der gegenüber Filmaufnahmen in anderen öffentlichen Bereichen eine besondere Eingriffsschwere aufwies. Auch die frei zugängliche Veröffentlichung besonders sensibler Information im Internet, beispielsweise von Informationen über Kinder oder von privaten Handynummern, erfordern aus unserer Sicht regelmäßig eine datenschutzaufsichtliche Ahndung mittels Geldbuße.

Verantwortliche der der ZBS gemeldeten datenschutzrechtlichen Verstöße waren jedoch nicht nur Privatpersonen, sondern vielfach auch Unternehmen. Diese Fälle gelangten überwiegend aufgrund interner Abgaben aus den LDA-Fachbereichen an die ZBS. Beispielhaft kann hier ein Fall angeführt werden, über den wir bereits in unserem 21. Tätigkeitsbericht berichtet haben. Ein Inkassobüro kontaktierte hier im Rahmen seiner Forderungsbearbeitung die Arbeitgeber:innen der Forderungsschuldner:innen, mit der Bitte, an ihre Beschäftigten heranzutreten und zu fragen, ob diese doch noch eine freiwillige Zahlung leisten würden (11. Tätigkeitsbericht 2021, Ziff. 9.2). Dieses Vorgehen wurde von

uns als unzulässig angesehen und beschäftigt mittlerweile auch die ZBS.

Ein qualitativ und quantitativ besonders schwerwiegender Fall betrifft ein Unternehmen, das bei einem Umzug in den früheren Büroräumen eine größere Zahl an Personalakten zurückgelassen hat, die von Beschäftigten der Nachmieterin dort aufgefunden wurden.

Auffallend war zudem eine Häufung von der ZBS gemeldeten Fällen aus dem Gesundheitsbereich. In mehreren Fällen führten Ärzt:innen oder Apotheker:innen Unterlagen mit sensiblen personenbezogenen Daten ohne vorherige datenschutzkonforme Vernichtung oder Behandlung der normalen Hausmüllentsorgung zu. Dies ist vor allem deshalb kritisch, weil die Unterlagen in der Regel Daten enthalten, die dem besonderen Schutz des Art. 9 DS-GVO unterfallen.

Die im Berichtsjahr eingeleitete Bußgeldverfahren konnten noch nicht alle abschließend bearbeitet werden, was zum Teil an vorrangigen staatsanwaltlichen Ermittlungen liegt, zum anderen aber auch mit den aktuell vom EuGH zu klärenden Grundsatzfragen der Zurechnung von Fehlverhalten bei juristischen Personen bei der Verhängung von Sanktionen nach Art. 83 DS-GVO (Rechtssache C-807/21).

Positiv hervorzuheben bleibt in diesem Zusammenhang die stets gute Kooperation mit den Staatsanwaltschaften und die gute Zusammenarbeit mit den Polizeibehörden, die die ZBS im Berichtszeitraum oftmals bei Ermittlungshandlungen unterstützten.

Im Berichtszeitraum veröffentlichte der Europäische Datenschutzausschuss die Leitlinien zur Berechnung von Geldbußen gemäß der DS-GVO. Das Konsultationsverfahren wurde noch vor der Veröffentlichung des Tätigkeitsberichts abgeschlossen und die Leitlinien von dem Europäischen Datenschutzausschuss angenommen (Guidelines 04/2022 on the calculation of administrative fines under the GDPR). Die Leitlinien sehen für die Festsetzung der Geldbuße eine einheitliche europäische Methodik vor und schaffen so eine klare und transparente Grundlage für die Festsetzung von Geldbußen durch die europäischen Aufsichtsbehörden. Sie tragen damit maßgeblich zur Harmonisierung zwischen den Mitgliedstaaten hinsichtlich der Höhe der Geldbußen bei, lassen gleichzeitig aber Spielraum für die konkrete Abwägung im Einzelfall.
Wesentliches Element der Leitlinien ist die Festlegung eines Grundbetrages für die Zumessung der Geldbuße, für den neben der Einordnung des Verstoßes in Art. 83 Abs. 4 bis 6 DS-GVO dessen Schwere und der Umsatz des Unternehmens relevant ist. Die Leitlinien unterscheiden dabei zwischen Verstößen geringen, mittleren und hohen Schweregrades und sehen zur Bestimmung des Ausgangsbetrages zunächst einen prozentualen Anteil des jeweils anwendbaren gesetzlichen Höchstbetrages vor, der sich nach der Schwere des Verstoßes richtet (bei Verstößen mittleren Schweregrades beispielsweise 10 bis 20 Prozent des gesetzlichen Höchstbetrages). Für den sich daraus ergebenen Betrag sieht die Leitlinie dann eine weitere Anpassungsmöglichkeit anhand des Unternehmensumsatzes vor - bei Kleinstunternehmen bis zu einem Umsatz von höchstens 2 Mio. Euro beispielsweise eine (weitere) Reduzierung auf 0,2 bis 0,4 Prozent, bei Unternehmen mit einem Jahresumsatz zwischen 100 und 250 Mio. Euro beispielsweise eine Reduktion auf 15 bis 50 Prozent des ermittelten Betrages. Der nach diesen Kriterien bestimmte Wert bildet schließlich den Ausgangsbetrag für die endgültige Festsetzung der Geldbuße, für die die weiteren erschwerenden und mildernden Umstände des Einzelfalls berücksichtigt werden und gegebenenfalls weitere Anpassung erfolgen, um sicherzustellen, dass die Geldbuße wirksam, abschreckend und verhältnismäßig ist.

Die in den Leitlinien festgelegte Methode ist für das LDA Grundlage für die Festsetzung von

Geldbußen und Maßstab bei grenzüberschreitenden Sachverhalten im Rahmen unserer Aufgaben im Kooperations- und Kohärenzverfahren um zu bewerten, inwieweit eine durch eine andere europäische Aufsichtsbehörde verhängte Geldbuße den Bewertungskriterien des Art. 83 DS-GVO entspricht.

Stichwortverzeichnis

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