Bayerisches Landesamt für
Datenschutzaufsicht

14. Tätigkeitsbericht

2024

14. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht
für das Jahr 2024

Herausgeber:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

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

Titelbild: Midjourney: female figure representing the Guardian of Fundamental Rights, wearing a flowing robe can is sitting at a table with a half-empty glass of water on it. she is looking interested at it. Background is filled by the European Union flag with its circle of 12 golden stars. --ar 16:9

Vorgelegt im März 2025 – Michael Will, Präsident

Datenschutz im Jahr 2024 – notwendig, aber nicht mehr selbstverständlich?

Ein Rückblick auf das Datenschutzjahr 2024 des BayLDA hinterlässt ein irritierend zwiespältiges Bild. Während es ohne allzu große Abstriche gelungen ist, durch zusätzliche Ressourcenspielräume notwendige strukturelle Umbauprozesse einzuleiten und nicht wenigen inhaltlichen Herausforderungen wie dem ersten europaweiten Großverfahren unter bayerischer Federführung (siehe hierzu auch Kapitel 14.1 zum Projekt „Worldcoin") gerecht zu werden, scheint sich in der politischen, ökonomischen und gesellschaftliche Wahrnehmung des Datenschutzes im Jahresverlauf 2024 ein Vorzeichenwechsel vollzogen zu haben.

Der „Guardian of a Fundamental Right", die Metapher der Datenschutzaufsichtsbehörden und ihres Schutzauftrags aus Art. 8 der EU-Grundrechtecharta, blickt daher diesmal versonnen-pessimistisch vom Titelbild des 14. Tätigkeitsberichts unserer Behörde auf ein nur halbvolles bzw. bereits halbleeres Glas.

Datenschutz als Standortfaktor oder –nachteil?

Datenschutz zu erklären und seine praktische Umsetzung zu vermitteln, zählt fraglos zu den Basisaufgaben der Datenschutzaufsicht. Prägend für das Jahr 2024 bleibt aber die Grunderfahrung in zahllosen großen und kleinen, öffentlichen und internen Diskussionsrunden, die Notwendigkeit des Schutzes personenbezogener Daten in einer zunehmend digitalisierten Gesellschaft nicht als selbstverständliches Gut voraussetzen zu dürfen, sondern sie rechtfertigen bzw. gar gegen den Vorwurf des Innovationshemmnisses und Standortbenachteiligung verteidigen zu müssen.

Ein branchen- und institutionenübergreifendes Grundnarrativ des Jahres 2024 war, auch vor dem Hintergrund wirtschaftlicher Krisen und weltpolitischer Spannungslagen, dass „Datenschutz verzichtbare, mindestens aber reformbedürftige Bürokratie" sei – vorgetragen vom bayerischen Unternehmensverbandsvertreter bis zum vormaligen EZB-Präsidenten und EU-Berater im seinem viel beachten „Draghi-Bericht" zur „Zukunft der Wettbewerbsfähigkeit der EU".

Datenschutz erst ermöglicht Datennutzung?

So notwendig die sorgfältige Auseinandersetzung mit solcher Kritik in jedem Einzelfall bleibt, so wenig überzeugt ein im Vorwurf der „Bürokratie" eingebetteter Kerngedanke. Mit dem Etikett der „Bürokratie" wird Datenschutz zum scheinbar politisch disponiblen regulatorischen Selbstzweck. Unabhängig von den durch Art. 8 der EU-Grundrechtecharta und Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union bestimmten unionsrechtlichen Rahmenbedingungen, verstellt die Formel „Datenschutz = Bürokratie" den Blick auf dessen elementare Bedeutung für das Gelingen der Digitalisierung in einer freiheitlichen Gesellschaft.

Datenschutzrechtliche Anforderungen zielen im Kern auf „Verantwortliche" und ihre „Verantwortlichkeit"; sie stellen die Frage der „Verantwortbarkeit" bestimmter Prozesse oder Technologien. Sie fordern unserem Verständnis nach von Unternehmen im Kern nichts anderes als Übersicht, Nachvollziehbarkeit und Kontrolle. Datenschutzrechtliche Anforderungen sind damit Gegenmodell zu einem undurchsichtigen und unverstandenen „plug and play", also dem ungeprüften Adaptieren von vermeintlich förderlichen, tatsächlich aber selbst große Organisationen bisweilen (über-)fordernden, hochkomplexen Technologien.

Gerade mit Blick auf den zunehmenden Einzug von Praxisanwendungen Künstlicher Intelligenz, die grundlegend noch weit mehr die Frage nach der menschlichen Kontrollierbarkeit und Verantwortbarkeit aufwerfen, erscheinen diese Grunderwartungen weder überbordend noch unproduktiv. Datenschutzrechtliche Verantwortbarkeit sichert vielmehr nachhaltige Übersicht und Kontrolle über Datenflüsse. Und schafft damit erst die Grundbedingung, sinnvoll über die künftige Nutzung von Daten, sei es durch das Teilen von Daten oder die interne Verwendung für Entwicklung oder bspw. auch Forschung wohlüberlegt entscheiden zu können.

Mittelbar wirken datenschutzrechtliche Anforderungen so auch der Verschiebung von Macht und Kontrolle zwischen Kunden und Anbietern, Technologienutzenden und Technologieanbietenden entgegen, indem sie Transparenz und Rollenzuweisungen einfordern bzw. Grenzen z. B. durch Zweckbindungserfordernisse setzen. Solche Anforderungen tragen letztlich auch zur Resilienz in Krisensituationen bei, indem sie die Übersicht und Kontrolle über Datenflüsse und die an ihnen beteiligten Akteure ermöglichen.

Bessere Bedingungen für selbst-verständlichen Datenschutz

Für das BayLDA war die Grundsatzdebatte des Jahres 2024 über die Notwendigkeit des Datenschutzes und seine angemessene Ausgestaltung und Handhabung Anlass und Motivation, sich breiter und intensiver als in den zurückliegenden Jahren für ein besseres Verständnis des Datenschutzes durch Unternehmen und Vereine in Bayern einzusetzen. Kaum eine Woche im Team-Kalender verzeichnet nicht mindestens eine Mitwirkung von Expertinnen und Experten unserer Behörde an Webinaren, Diskussionsrunden oder Erfa-Kreisen vor Ort bis hin zu den großen deutschen oder europäischen Fachveranstaltungen, um Wissen zu vermitteln, aktuelle Entwicklungen zu erläutern oder konkrete Fragen und Anliegen aufzugreifen. Parallel dazu haben wir eine umfassende Aktualisierung unserer Informationsangebote eingeleitet, die nun insbesondere im Bereich der KI-Nutzung mit praxisorientierten Handreichungen Vorbehalten entgegenwirken und Innovationsentscheidungen unterstützen sollen.

2025 – ein Jahr der Weichenstellungen?

Erste Rückmeldungen auf unsere Informationskampagnen zeichnen ein ermutigendes Bild, wenngleich sie im Berichtszeitraum noch zu keinem statistisch erfassbaren Anstieg bei individuellen Beratungsanfragen geführt haben (siehe hierzu auch Kapitel 2.2 und 2.3).

Bei der Fortführung unserer Aufklärungs- und Sensibilisierungsmaßnahmen für Unternehmen und Vereine genauso, wie für die Erfüllung unserer übrigen Aufgaben zur unionsweit einheitlichen Durchsetzung der DS-GVO bleibt freilich im Blick zu behalten, dass jedenfalls für die EU-Digitalrechtsakte, insbesondere für die KI-Verordnung und die zentralen Bestimmungen der sog. Datenverordnung (Data Act) spätestens in der zweiten Jahreshälfte 2025 durch den Bundesgesetzgeber nationale Zuständigkeitsregelungen getroffen werden müssen. Die noch vor den Bundestagswahlen bekannt gewordenen Regelungsvorschläge der zuständigen Ressorts sahen dafür bislang übereinstimmend zentrale Zuständigkeiten von Bundesbehörden auch im Bereich des nicht-öffentlichen Datenschutzes vor. Weitergehende Reformvorschläge fordern darüber hinaus, die Wahrnehmung der Datenschutzaufsicht gegenüber Unternehmen und Vereinen insgesamt von den Datenschutzaufsichtsbehörden der Länder auf den Bund zu übertragen. Ob und inwieweit diese Vorschläge durch den neu gewählten Bundestag unterstützt und vom Bundesrat im Rahmen seiner föderalen Mitwirkungsrechte gebilligt werden, ist zum Zeitpunkt der Vorlage dieses Berichts nicht absehbar. Bis dahin werden wir im Rahmen unserer datenschutzaufsichtlichen Bera-

tungsaufgaben gegenüber Regierung und Parlament alle Möglichkeiten nutzen, für die Vorzüge föderaler Zuständigkeitsstrukturen für Unternehmen und Betroffene zu werben und ihre Leistungsfähigkeit unter Beweis zu stellen.

Ansbach, im März 2025

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

1.2 Datenschutz in Bayern

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

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

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

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

1.3 Das Bayerische Landesamt für Datenschutzaufsicht

Die Personalausstattung des BayLDA ist im Berichtszeitraum auf nominell 38 Planstellen angewachsen. Aufgrund des konstant hohen Niveaus der Beschwerdezahlen und der generellen Aufgabenmehrung, gerade auch im Hinblick auf die datenschutzrechtliche Beurteilung des Einsatzes von KI- Systemen, wurden vom BayLDA noch für die Haushaltsaufstellung 2024/25 insgesamt 47 neue Planstellen angemeldet. Mit der Ausbringung von insgesamt 10 neuen Planstellen für den Doppelhaushalt 2024/2025, hat der Haushaltsgesetzgeber zwar weiterhin erhebliche Kompromisse und Priorisierungszwänge bei der Erfüllung datenschutzaufsichtlicher Aufgaben

für erforderlich erachtet. Erstmals seit Geltungsbeginn der Datenschutz-Grundverordnung werden damit aber Strukturveränderungen ermöglicht, die es zumindest erlauben, den aktuellen Handlungserfordernissen nachzukommen. Auch wenn die Hälfte der zusätzlichen Planstellen faktisch erst zum Jahresende 2025 besetzbar sein wird, ergeben sich dennoch in der Gesamtschau spürbare zusätzliche organisatorische Spielräume. Sie erlauben es insbesondere, den mit den EU-Digitalrechtsakten verbundenen datenschutzrechtlichen und -technischen Fragen oder der Begleitung der digitalen Transformation in Industrie, Wirtschaft und Handwerk durch verstärkte Beratung jedenfalls ansatzweise Rechnung zu tragen.

Im Mittelpunkt dieser Umstrukturierung steht die Etablierung eines KI-Beauftragten. Damit will das BayLDA der strategischen Bedeutung von KI im Technologieland Bayern Rechnung tragen und besonders Rechtssicherheit bei der KI-Nutzung bei kleinen und mittleren Unternehmen (KMU) schaffen. Auch bei Datenschutzkontrollen – ob anlassbezogen oder anlasslos – wird diese Rolle mit ihrem internen KI-Fachwissen unterstützend tätig sein. Für rechtliche Fragen zur Künstlichen Intelligenz steht zusätzlich der neue Fachbereich "Digitalwirtschaft" im BayLDA bereit. Dort werden zudem, neben dem klassischen Datenschutz im Internet, auch datenschutzrechtliche Fragestellungen im Rahmen von Beschwerde- oder Beratungsanfragen im Bereich der personenbezogenen Datennutzung wie z. B. im Rahmen der Anwendung der Datenverordnung (DataAct) bearbeitet. Mit diesem Teamwork fühlt sich das BayLDA für die aktuellen und künftigen Herausforderungen im KI-Bereich und Digitalrechtsakte zumindest vorerst bestens gerüstet.

Personalverstärkungen bzw. -Umschichtungen sollen auch die, durch den KI-Beauftragten begleite interne Entwicklung und den Einsatz von KI im LDA voranbringen. Mittelfristig wird dazu auch das LDA-Verwaltungsprogramm IGOR einen eigenen, vor Ort betriebenen KI-Assistenten erhalten. Einzelheiten der Neuorganisation sind aus dem Organigramm des BayLDA ersichtlich:

Bereich G Hr. Filip	Bereich 1 Hr. Baer – Hr. Will	Bereich 2 Fr. Lipps	Bereich 3 Fr. Loy	Bereich 4 Hr. Sachs	Bereich 5 Fr. Meder	Bereich Z Fr .Drechsel
Geschäftsleitung Geschäftsstelle, Bürgertelefon: Leitung: Fr. Küchle Stabstelle für europäische Zusammenarbeit Grundsatzfragen, insbesondere Recht der Auftragsverarbeitung; Internationaler Datenverkehr	Wohnungswirtschaft Industrie und Handel Vereine Kredit- und Finanzwirtschaft Auskunfteien Datenschutzbeauftragte	Gesundheitswesen Versicherungen Soziale Einrichtungen Freiberufliche Tätigkeiten	Digitalwirtschaft	• Beschwerden, Cybervorfälle, Datenpannen • Beratungen, organisator. Datenschutz, techn. Gremien-arbeit • Zertifizierungen • Cyber-/IT-Labor, eGovernment • Automotive, DSFA	Beschäftigten-datenschutz Videoüberwachung Werbung, Kunden-bindungssysteme Markt- und Meinungsforschung	Justiziariat, Zentrale Bußgeldstelle

2

Zahlen und Fakten

2 Zahlen und Fakten

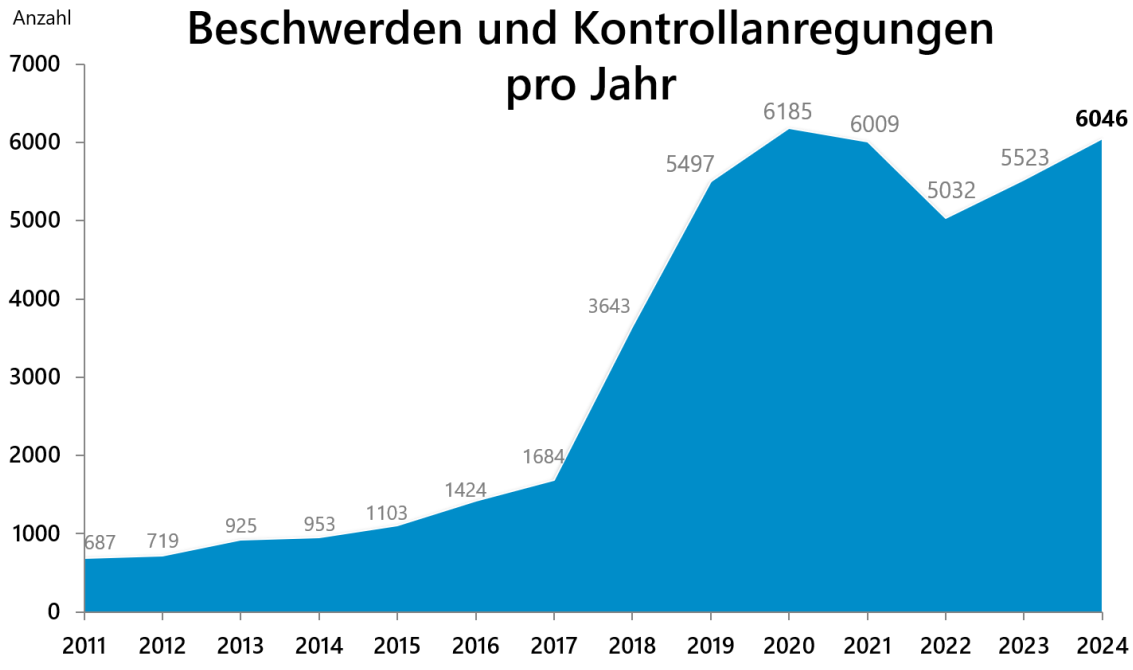
Die Bearbeitung von Datenschutzbeschwerden und Meldungen von Sicherheitsverletzungen beanspruchte auch in 2024 einen überwiegenden Teil unserer Ressourcen:

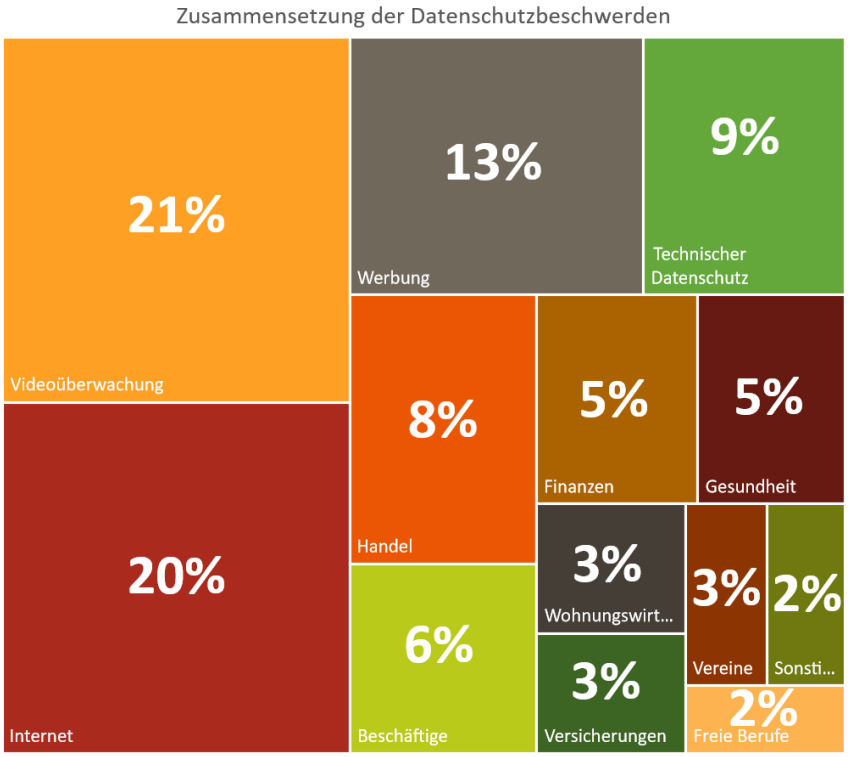
2.1 Beschwerden

Die Gesamtanzahl der Beschwerden und Kontrollanregungen, die 2024 bei uns eingegangen sind, ist der unten folgenden Grafik zu entnehmen. Mit einem ca. siebenprozentigen Anstieg der Eingangszahlen haben wir das Allzeithoch aus 2020 wieder nahezu erreicht.

Die Schwerpunkte der Bearbeitung haben sich gegenüber dem Vorjahr nicht spürbar verändert. Beschwerden im Bereich Videoüberwachung führen die Statistik mit ca. 21 % auch 2024 an und bilden zusammen mit Beschwerden aus dem Bereich Internet (20 %) und dem Bereich „Werbung“ (14 %) mehr als die Hälfte aller Vorgänge im BayLDA ab (siehe Grafik nachfolgende Seite).

Als Beschwerden werden dabei nach wie vor solche Vorgänge gezählt, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt, für die Art. 77 DS-GVO anwendbar ist. Dies schließt Abgaben von anderen Behörden ein.

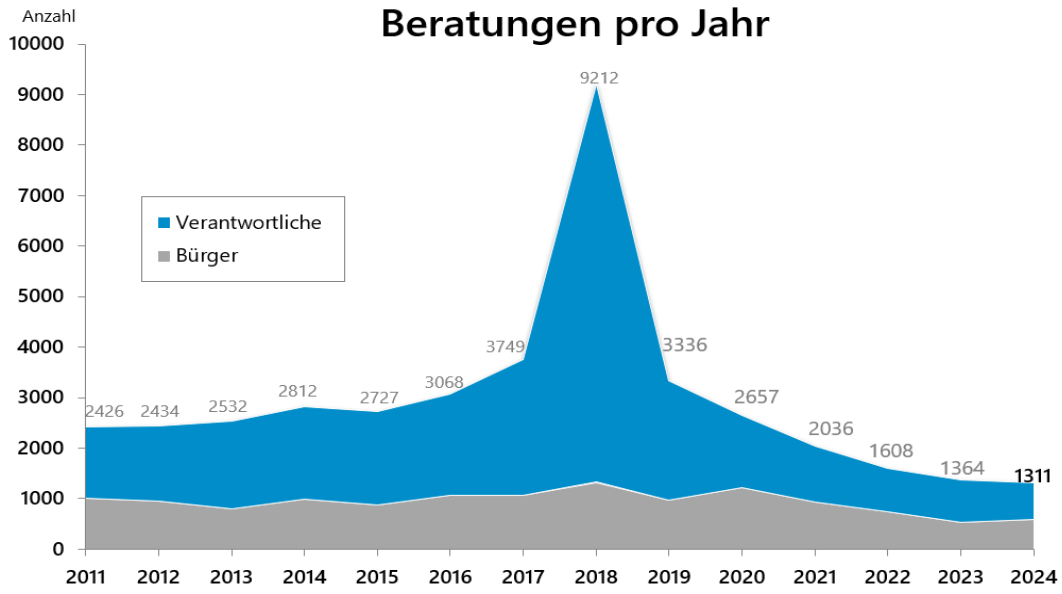




2.2 Beratungen

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 sowie der Staatsregierung (Art. 57 Abs. 1 c) und d) DS-GVO), außerdem telefonische Beratungen, die im Vorgangsverwaltungssystem erfasst wurden. Schulungen, Vorträge etc. werden nicht mehr berücksichtigt, aber derzeit dennoch von uns separat erfasst.

In der nachstehenden Grafik sind die Beratungen im Berichtszeitraum aufgeführt. Sie umfasst wie in den Vorjahren auch telefonische Beratungen im eben genannten Sinne.



Hier zeigt sich mit nur noch ca. 1311 Beratungen ein Allzeit- Tief, welches aus unserer Sicht allerdings nicht dem Mangel an Anfragen, sondern der weiterhin bestehenden Personalknappheit geschuldet ist. In den Vorjahren war zu selten eine rechtzeitige und bedarfsgerechte Beratung von datenschutzrechtlichen Anliegen möglich. Zeitweise musste wir deshalb sogar unser generelles Beratungsangebot auf unserer Homepage entfernen und uns auf die gesetzlichen Mindestaufgaben wie die Beratung von betrieblichen Datenschutzbeauftragten beschränken.

In der zweiten Jahreshälfte 2024 konnte diese unzufriedenstellende Situation unserer durch den Sensibilisierungsauftrag der DS-GVO geforderten Beratungsangebote allerdings dank der mit dem Stellenzuwachs im Doppelhaushalt 2024/25 eröffneten Handlungsspielräume zumindest in einem ersten Schritt korrigiert werden (s. Grafik mit einem Auszug aus unserem online-Beratungsangebot). Inwieweit dieses reaktivierte Beratungsprogramm angenommen wird, werden die Statistiken des Datenschutzjahrs 2025 zeigen.

2.3 Spezielle neue Beratungen

KI- Beratung

Gerade im Hinblick darauf, dass zum Ende des Berichtszeitraums noch keine Marktüberwachungsbehörde im Sinne von Art. 77 KI-VO in Deutschland benannt wurde, fehlt es hier derzeit noch an einer Anlaufstelle für betroffene Unternehmen. Dies unterscheidet sich stark von der DS-GVO-Einführung zwischen 2016 und 2018, während der die bestehenden deutschen Datenschutzbehörden umfassend beraten konnten. Dieser Bereich wurde deshalb im Rahmen des Neustarts unseres Online-Beratungsangebots zusätzlich aufgenommen

Daher ist es unser Ziel, gerade im Hinblick auf die entscheidenden Schnittstellen zwischen Datenschutz und KI, Verantwortliche im Rahmen unserer Kompetenzen zu beraten und zu unterstützen, um Innovationen zu fördern und Rechtsunsicherheiten vorzubeugen. Wir planen für 2025 unsere KI-Beratung durch datenschutzbezogene Schulungen, Beratungen etc. auszubauen, da auf Grund der vorgezogenen Bundestagswahlen die Klärung der Zuständigkeit für die KI-Marktüberwachung und deren Umsetzung erst in der zweiten Jahreshälfte 2025 zu erwarten ist.

Cyberprävention

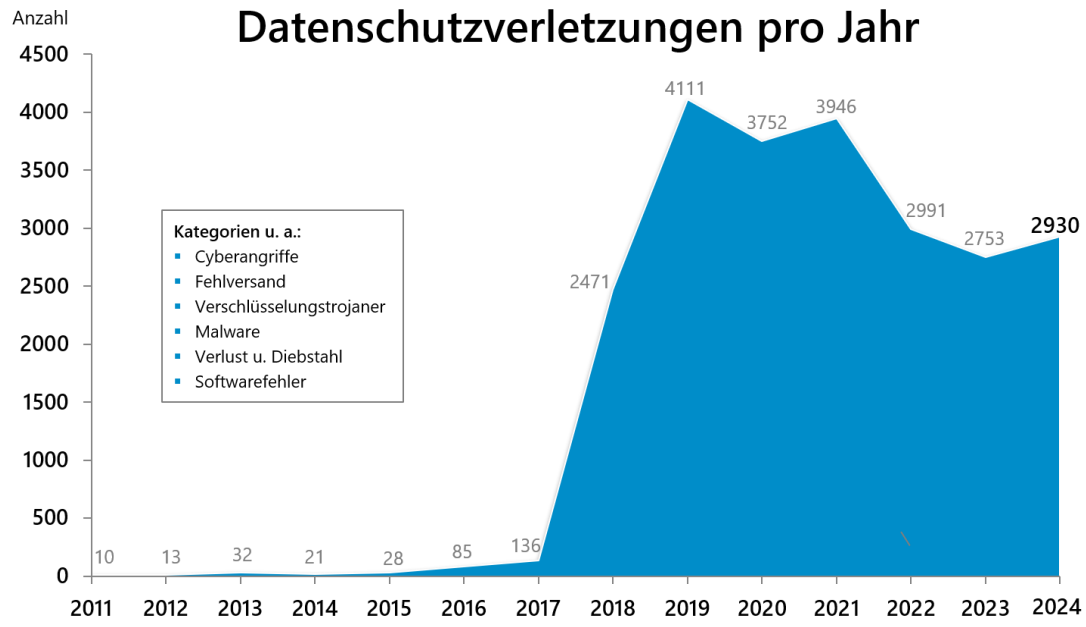
Daneben hat die weiter hohe Bedrohungslage im Bereich Cybersicherheit einen zweiten neuen Beratungsschwerpunkt, die Rubrik „Cyberpräventions-Beratung“ erforderlich gemacht (siehe hierzu auch Kapitel 14.2).

Wir vertreten die Auffassung, dass möglicherweise bis zu 80 Prozent aller Cyberangriffe mit bekannten und leicht verfügbaren technischen und organisatorischen Maßnahmen verhindert werden könnten. Daher wollen wir gerade den Fokus auf diese leicht umsetzbaren und nicht mit hohem Kostenaufwand verbundenen Maßnahmen legen und durch Checklisten, Informationsangebote, aber auch individuelle Beratung dazu beitragen, dass gerade kleine und mittlere Unternehmen besser geschützt sind und Angriffen standhalten können.

2.4 Datenschutzverletzungen

Im Gegensatz zu den Vorjahren ist die Zahl der Meldungen von Verletzungen der Sicherheit bei der Verarbeitung personenbezogener Daten 2024 wieder angestiegen. Auffällig ist dabei, dass der Anteil an Cybersicherheitsvorfällen weiter spürbar zunimmt. Täglich erreichen das BayLDA Meldungen über Cyberattacken - von Ransomware-Angriffen auf produzierende Mittelstandsbetriebe bis hin zu gehackten E-Mail-Accounts bei kleineren Einrichtungen wie bspw. Arztpraxen. Erkennbar ist, dass die kriminellen Akteure längst vor niemanden mehr Halt machen und auch Organisationen aus dem KRITIS und Sub-KRITIS-Spektrum ins Visier nehmen, aber auch Kindergärten, Schulen, Pflege- und Sozialeinrichtungen sowie Kliniken. So mögen Schäden bei sozialen und medizinischen Einrichtungen letztlich in vielen Fällen zwar wirtschaftlich verkraftbar sein, jedoch sind die Schäden für die vom Vorfall betroffenen Personen wie bspw. Patienten meist enorm. Dagegen zielen Angriffe auf finanzstarke Unternehmen primär weiter auf die Zahlung sehr hoher Lösegeldforderungen ab - oftmals im sechs- oder siebenstelligen Euro-Bereich, wenn man die Bitcoin-Kurse umrechnet. Insgesamt wird deutlich, dass Cybersicherheitsmaßnahmen nicht nur für den Schutz personenbezogener Daten förderlich sind, sondern auch eine notwendige Absicherung der eigenen Wirtschaftsverhältnisse darstellen. Details zur Cybersicherheitslage finden sich im Kapitel 15 dieses Tätigkeitsberichts.

Abseits der registrierten Cybersicherheitsvorfälle scheint es, als würden manche Betriebe



eine gewisse Routine in der Meldung von Vorfällen wie Fehlversendungen, Buchungsfehlern oder Verlustsachen entwickeln - und andere Verantwortliche ihrer Meldeverpflichtung allerdings überhaupt nicht nachkommen. Gerade innerhalb von Branchen zeigt sich daher ein sehr heterogenes Bild, was das Meldebewusstsein und die Meldemoral anbelangt. Entsprechend findet hier das BayLDA regelmäßig Anknüpfungspunkte für gezielt angelegte Datenschutzprüfungen.

3

Europäische Zusammenarbeit

3 Europäische Zusammenarbeit

3.1 Verfahren der Zusammenarbeit und Kohärenz

Die Mitwirkung an grenzüberschreitenden Verfahren gehört für das BayLDA auch weiterhin zum Alltag.

Wie bereits in den vorangegangenen Jahren, nahmen auch 2024 Verfahren der Zusammenarbeit und der Kohärenz mit den anderen europäischen Datenschutzaufsichtsbehörden wichtigen Raum in unserer aufsichtlichen Tätigkeit ein. Die vom Gesetz vorgesehenen Verfahren der Zusammenarbeit und Kohärenz hatten wir in unseren beiden letzten Tätigkeitsberichten ausführlich dargestellt.

Bayern ist ein wichtiger Wirtschaftsstandort und beherbergt Niederlassungen vieler grenzüberschreitend tätiger Unternehmensgruppen, daher ist unser Haus in überproportionalem Maße an datenschutzaufsichtlichen Verfahren beteiligt, die im Zusammenarbeitsverfahren mit anderen europäischen Datenschutzbehörden zu bearbeiten sind.

Im Berichtszeitraum waren wir an 521 europäischen Zusammenarbeitsverfahren beteiligt, davon 131 neuen Verfahren, für die unser Haus die Rolle der federführenden Aufsichtsbehörde innehatte. Ein öffentlich bekanntes Beispiel ist das World(coin)- Verfahren, siehe hierzu unter Kapitel 14.1.

Darüber hinaus betreuten wir 80 neue Verfahren, in denen wir sog. betroffene Aufsichtsbehörde nach Art. 4 Nr. 22 DS-GVO waren. 40 Zusammenarbeitsverfahren haben wir als federführende Aufsichtsbehörde im Berichtszeitraum abgeschlossen.

Aufgrund der laufend weiter zunehmenden praktischen Erfahrungen der Aufsichtsbehörden mit dem Zusammenarbeitsverfahren konnte die Effizienz der Kooperation in den letzten Jahren stetig verbessert werden. Damit ist das in der DS-GVO verankerte Modell des gemeinsamen Vollzugs eines europäischen Rechtsakts durch die Aufsichtsbehörden der EU-Mitgliedstaaten im Datenschutz heute gelebte Realität und gehört auch für unser Haus zum Alltag. Nichtsdestotrotz bleiben bei den europäischen Zusammenarbeitsverfahren noch Herausforderungen, die sich nicht nur aus der großen Anzahl der Fälle, sondern zum Teil auch aus Unterschieden in den Verfahrensrechtsordnungen der Mitgliedstaaten ergeben. In der täglichen Praxis ist es ungeachtet dessen in vielen Fällen gelungen, gemeinsame, von allen Aufsichtsbehörden mitgetragene Lösungen auch in Verfahrensfragen zu finden. Nicht zuletzt trugen dazu auch Entscheidungen des Europäischen Datenschutzausschusses bei.

3.2 Mitwirkung in Subgroups des EDSA

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

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

der DS-GVO weitestgehend übernommen – lediglich kleinere Änderungen wurden durchgeführt

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

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

Im Berichtszeitraum stellten wir weiterhin den Landesvertreter in der International Transfer Expert Subgroup. 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 insbesondere die Berichterstattung für die noch nicht abgeschlossene Arbeit an dem Papier „Recommendations for BCR-Processors“, sowie an der Opinion des EDSA zu „Consent or pay“- Modellen und die derzeit noch in Arbeit befindlichen Guidelines zu dieser Thematik.

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

4

Allgemeines und Betroffenenrechte

4 Allgemeines und Betroffenenrechte

4.1 Erstes Vorabentscheidungsverfahren unter Beteiligung des Bayerischen Landesamts für Datenschutzaufsicht

Art. 20 Abs. 2 Bayerisches Datenschutzgesetz (BayDSG) auf dem Prüfstand

Das Verwaltungsgericht Ansbach hat sich in einem bereits mehr als zwei Jahre andauernden Verfahren entschieden, zu Grundsatzfragen eine Vorabentscheidung des Europäischen Gerichtshofs (EuGH) einzuholen.

Geklagt hatte ein Beschwerdeführer, der nach Erhalt der Abschlussmitteilung bei uns einen Anspruch auf Auskunft nach Art. 15 DS-GVO und hilfsweise Akteneinsicht geltend gemacht hatte, weil ihm unsere Angaben zu den ergriffenen Maßnahmen nach Art. 58 DS-GVO nicht konkret genug waren. Beide Anträge wurden von uns mit Verweis auf Art. 20 Abs. 2 BayDSG, welcher Auskunfts- oder Einsichtsrechte hinsichtlich Akten und Dateien der Aufsichtsbehörden verwehrt, abgelehnt.

Der Kläger hält die Vorschrift im Bayerischen Datenschutzgesetz (BayDSG) für unionsrechtswidrig und verfolgte seinen Anspruch auf Auskunft, allerdings beschränkt auf den Beschwerdevorgang, gerichtlich weiter. Er begründete die Klage im Wesentlichen damit, dass Art. 20 Abs. 2 BayDSG die Voraussetzungen der Öffnungsklausel des Art. 23 DS-GVO nicht erfüllt, die es zwar grundsätzlich ermöglicht, die Betroffenenrechte wie das Auskunftsrecht einzuschränken, nach Auffassung des Klägers aber Art. 20 Abs. 2 BayDSG in dieser Form nicht rechtfertigen kann. Aufgrund der zwischenzeitlich ergangenen Rechtsprechung des EuGH, die sog. „Schufa-Entscheidung" (Urteil vom 07.12.2023 in den verbundenen Rechtssachen Az.: C-26/22 und C-64/22) wurde dem Kläger noch während des laufenden Klageverfahrens – ohne weitere Berufung auf Art. 20 Abs. 2 BayDSG – vollumfänglich Einsicht in die Beschwerdeakte gewährt. An seiner Klage hielt er – nunmehr in Form einer sog. Fortsetzungsfeststellungsklage – fest und trug vor, die Absicht zu haben, auch künftig Auskunftsersuchen gegen Datenschutzaufsichtsbehörden zu richten. Das Verwaltungsgericht Ansbach sah hierin eine Wiederholungsgefahr und legte dem EuGH im Rahmen eines Vorabentscheidungsersuchens folgende Fragen vor:

> *„1. Ist Art. 15 VO (EU) 2016/679 i. V. m. Art. 4 Nr. 7 VO (EU) 2016/679 dahingehend auszulegen, dass eine Aufsichtsbehörde nach Art. 4 Nr. 21 VO (EU) 2016/679, die im Rahmen eines von einer betroffenen Person eingeleiteten Beschwerdeverfahrens nach Art. 77 VO (EU) 2016/679 tätig wird, gleichzeitig im Sinne von Art. 15 VO (EU) 2016/679 i. V. m. Art. 4 Nr. 7 VO (EU) 2016/679 „Verantwortlicher" und damit auf Grundlage des Art. 15 VO (EU) 2016/679 gegenüber der betroffenen Person zur Auskunft verpflichtet ist?*
>
> *2. Für den Fall, dass Frage 1 mit „ja" beantwortet wird:*
>
> *Ist das Unionsrecht, insbesondere Art. 23 VO (EU) 2016/679, dahingehend auszulegen, dass es einer nationalen Regelung – wie dem im Ausgangsverfahren streitigen Art. 20 Abs. 2 BayDSG – entgegensteht, wonach Auskunfts- oder Einsichtsrechte hinsichtlich Akten und Dateien der Aufsichtsbehörden nach Art. 4 Nr. 21 VO (EU) 2016/679 pauschal nicht bestehen?"*

Die Vorschrift im Bayerischen Datenschutzgesetz, wonach Auskunfts- und Einsichtsrechte hinsichtlich Akten und Dateien der Aufsichtsbehörden nicht bestehen, versucht das Spannungsfeld zu lösen, in dem sich Datenschutzaufsichtsbehörden regelmäßig befinden:

Auf der einen Seite steht ein Verantwortlicher, der durch die den Aufsichtsbehörden zur Verfügung stehenden Befugnisse und der Anforderungen des Art. 31 DS-GVO zu einer umfassenden Mitwirkung und Offenlegung sämtlicher für die Prüfung erforderlicher Informationen verpflichtet werden kann. Der Durchsetzung dieser Mitwirkungspflichten kann mit Zwangs- und sogar Bußgeld Nachdruck verliehen werden und dazu führen, dass von dem Verantwortlichen vertrauliche Informationen offenbart werden müssen und diese so zum Aktenbestandteil werden. Auf der anderen Seite steht ein Beschwerdeführer, dem als Beteiligter in dem Verfahren möglicherweise ein Anspruch auf Akteneinsicht und als „betroffene Person" ein Anspruch auf Auskunft nach Art. 15 DS-GVO zuzubilligen ist. Nicht immer genügen hier die Vorschriften der Art. 29 Abs. 2, 30 BayVwVfG und Art. 15 Abs. 4 DS-GVO um die Vertraulichkeit von Informationen zu gewährleisten, die eine Datenschutzaufsichtsbehörde nicht zuletzt aufgrund der in Art. 54 Abs. 2 DS-GVO normierten Verschwiegenheitspflicht sicherzustellen hat. Diesem Spannungsverhältnis soll Art. 20 Abs. 2 BayDSG im Wesentlichen Rechnung tragen.

Die Vorschrift schützt neben dem Verantwortlichen aber auch vertrauliche Informationen des Beschwerdeführers oder anderer Betroffener vor einer Offenlegung durch Akteneinsichtsgesuche oder Auskunftsansprüche von Verantwortlichen und sichert auch insoweit die vom Verordnungsgeber vorgesehene Verschwiegenheitspflicht von Datenschutzaufsichtsbehörden und deren effektive und ordnungsgemäße Aufgabenerfüllung.

Neben der Frage, ob Art. 20 Abs. 2 BayDSG den Anforderungen an die Öffnungsklausel des Art. 23 DS-GVO gerecht wird und damit in der Lage wäre, gegen Datenschutzaufsichtsbehörden gerichtete Auskunftsansprüche nach Art. 15 DS-GVO vollständig und unbefristet auszuschließen, stellt sich hier zunächst die grundsätzliche Frage, ob eine Aufsichtsbehörde in dem Verhältnis zu einem Beschwerdeführer, der noch dazu ausdrücklich lediglich Auskunft aus einem Beschwerdevorgang erhalten möchte, überhaupt Verpflichteter eines Auskunftsanspruches nach Art. 15 DS-GVO sein kann: Die DS-GVO bestimmt unter Benennung und Definition der jeweiligen Normadressaten in Art. 4 DS-GVO Rechte und Pflichten der an einer Datenverarbeitung Beteiligten sowie der betroffenen Aufsichtsbehörden. Art. 15 DS-GVO richtet sich nach seinem ausdrücklichen Wortlaut an den Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO, nicht dagegen an die Aufsichtsbehörde nach Art. 4 Nr. 21 DS-GVO. Dass bei den sich aus der DS-GVO ergebenden Verpflichtungen danach differenziert werden muss, an welchen Adressaten sich diese richtet, sah auch das Verwaltungsgericht München in seinem Beschluss vom 24.03.2021, Az. M 13 K 20.6765 so. Hinzu kommt, dass die Pflichten der Aufsichtsbehörden in einem Beschwerdeverfahren – und damit einhergehend auch die Rechte des Beschwerdeführers – abschließend in den Art. 77 und 78 DS-GVO geregelt sind. Nach Art. 77 Abs. 2 DS-GVO sind die Rechte des Beschwerdeführers darauf beschränkt, über den Stand und das Ergebnis der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs unterrichtet zu werden. Weitergehende Auskunftsansprüche werden diesem hierin aber gerade nicht zugebilligt. Auch sieht die DS-GVO keine dem Art. 15 DS-GVO vergleichbare Vorschrift, die sich an Aufsichtsbehörden richtet, vor. Darüber hinaus verpflichtet (eigentlich) schon Art. 54 Abs. 2 DS-GVO Datenschutzaufsichtsbehörden zur Verschwiegenheit, was weiter die Frage aufwirft, ob es eines Rückgriffs auf Art. 20 Abs. 2 BayDSG überhaupt bedarf oder die Offenlegung vertraulicher Informationen nicht schon unter Verweis auf Art. 54 Abs. 2 DS-GVO abgelehnt werden muss. Wir gehen davon aus, dass der EuGH nun Klarheit in diese umstrittenen Fragen bringen und die Unionrechtskonformität von Art. 20 Abs. 2 BayDSG abschließend klären wird.

4.2 Kontrollpflichten bei Auftragsverarbeitung

Der Europäische Datenschutzausschuss hat die Kontrollverantwortung des Verantwortlichen bei Einschaltung von Auftrags- und Unterauftragsverarbeitern betont und für die Praxis näher erläutert.

Fragen zur Auftragsverarbeitung gehören in der Praxis der betrieblichen Datenschutzbeauftragten zu den Häufigsten. Gerade im Zusammenhang mit unserer Beratungsaufgabe gegenüber Datenschutzbeauftragten haben wir daher ein sehr zahlreiches Aufkommen von Fragen zu diesem Themenkomplex.

Insbesondere Kettenauftragsverhältnisse sind häufig Gegenstand der Fragestellungen. Also Sachverhalte, bei denen ein Auftragsverarbeiter seinerseits einen oder mehrere Unterauftragsverarbeiter (sog. weitere Auftragsverarbeiter) einschaltet. Dies ist gemäß Art. 28 Abs. 2 DS-GVO nur mit Zustimmung des Verantwortlichen möglich. Eine der entscheidenden datenschutzrechtlichen Fragen lautet damit, welche Kontrollpflichten den Verantwortlichen in derartigen Kettenauftragsverhältnissen treffen und wie die Auftragskontrolle ausgeübt werden kann bzw. muss.

Die dänische Datenschutzaufsichtsbehörde hat zu einer Reihe von Einzelfragen in diesem Zusammenhang eine Stellungnahme des Europäischen Datenschutzausschusses (EDSA) eingeholt (Stellungnahme 22/2024 des EDSA vom 07.10.2024). Diese liefert für die Praxis nun zahlreiche wertvolle Klarstellungen.

Betont hat der EDSA zunächst, dass der Verantwortliche während des gesamten Zeitraums, in dem eine Verarbeitung stattfindet, die Identität aller Auftragsverarbeiter und Unterauftragsverarbeiter kennen muss. Dies schon deshalb, weil der Verantwortliche bei Auskunftsersuchen betroffener Personen verpflichtet ist, alle konkreten Datenempfänger zu nennen, vgl. EuGH, Urt. v. 12.01.2013, C-143-21.

Eine weitere wichtige Klarstellung betrifft die Frage, inwieweit der Verantwortliche in einer Auftragskette die von den Unterauftragsverarbeitern zu erbringenden „hinreichenden Garantien", für technische und organisatorische Maßnahmen, selbst prüfen muss. Der EDSA betont, dass die DS-GVO in Art. 24 Abs. 1 und Art. 28 Abs. 1 letztlich dem Verantwortlichen die Verantwortung für die Datenschutzkonformität der gesamten Verarbeitung auferlegt und diese Verantwortung durch die Einschaltung von Auftragsverarbeitern und ggf. Unterauftragsverarbeitern nicht gemindert wird und unabhängig von der Zahl und Komplexität der Auftrags- und Unterauftragsverhältnisse gilt.

In der Praxis wird häufig gefragt, welches Ausmaß an Prüfung der Verantwortliche selbst leisten muss und inwieweit er ggf. die Prüfung der Garantien von Unterauftragsverarbeitern auf die „übergeordneten" Auftragsverarbeiter delegieren kann. Laut EDSA hängen Umfang und Detailgrad der vom Verantwortlichen selbst zu leistenden Kontrolle durchaus vom Risiko der jeweiligen Verarbeitung für betroffene Personen ab. Je höher das Risiko, desto mehr Auftragskontrolle muss der Verantwortliche selbst leisten, so dass dieser ggf. auch gehalten sein kann, einzelne Unterauftragsverträge selbst zu prüfen und sich nicht immer alleine auf die Prüfung durch den übergeordneten Auftragsverarbeiter verlassen kann. Insbesondere dann, wenn Auffälligkeiten oder Lücken hinsichtlich der Garantien oder deren Umsetzung bei einem Unterauftragsverarbeiter erkennbar werden, muss der Verantwortliche in aller Regel weitere Nachforschungen anstellen.

Der Verantwortliche hat jederzeit das Recht, vom Auftragsverarbeiter die Vorlage aller von diesem abgeschlossenen Unterauftragsverträge zu verlangen. Dies wird vom EDSA betont, auch wenn es – wie auch unsere Erfahrungen zeigen

- in der Praxis gelegentlich in Zweifel gezogen wird. Zwar ist der Verantwortliche nach Ansicht des EDSA nicht verpflichtet, systematisch von vornherein alle Unterauftragsverträge herauszuverlangen und selbst zu prüfen; allerdings wird dies in der Regel spätestens dann notwendig, wenn irgendwelche Zweifel mit Blick auf die Garantien beim Unterauftragsverarbeiter auftreten. Darüber hinaus kann es für Verantwortliche auch in anderen Fällen empfehlenswert sein, sich die Unterauftragsverträge vorlegen zu lassen und die technischen und organisatorischen Maßnahmen zu prüfen, um so nachzuweisen, dass sie ihrer Pflicht aus Art. 28 Abs. 1 DS-GVO nachgekommen sind.

Häufig kommt es im Rahmen von Auftragsverarbeitung zur Übermittlung personenbezogener Daten in Drittländer („Transfer"), weil einer oder mehrere der Auftrags- oder Unterauftragsverarbeiter in einem Drittland ansässig sind. Auch für diese Szenarien hat sich der EDSA zu den Kontrollpflichten des Verantwortlichen geäußert und die grundsätzliche datenschutzrechtliche Verantwortlichkeit des Verantwortlichen dafür betont, dass jeglicher Datentransfer in der Auftragskette die Anforderungen des fünften Kapitels der DS-GVO wahrt. Sofern die Daten an einen Auftrags- oder Unterauftragsverarbeiter in einem Drittland übermittelt werden, für das durch Beschluss der Europäischen Kommission ein sog. angemessenes Datenschutzniveau anerkannt ist, muss der Verantwortliche das Datenschutzniveau beim Datenempfänger nicht weiter prüfen, da dies durch den Kommissionsbeschluss bereits geleistet worden ist. Anders ist es bei Transfers an Empfänger in Drittländer ohne angemessenes Datenschutzniveau; hierfür werden in der Praxis meist sog. geeignete Garantien verwendet, etwa Standarddatenschutzklauseln, die mit dem Datenempfänger im Drittland abgeschlossen werden und zudem muss ein sog. Transfer Impact Assessment (TIA) durchgeführt werden. Bei letzterem wird die Rechtslage im Empfängerland dahingehend geprüft, ob sie den Empfänger daran hindern könnte, seine Verpflichtungen etwa aus den Standarddatenschutzklauseln einzuhalten, etwa weil Sicherheitsbehörden des Drittlands in einem unverhältnismäßigen Umfang Zugang zu den Daten erhalten könnten. Bei Auftragsketten wird der TIA häufig nicht vom Verantwortlichen, sondern von einem der in der Europäischen Union ansässigen Auftragsverarbeiter durchgeführt, der seinerseits die Daten (im Auftrag des Verantwortlichen) an einen Unterauftragsverarbeiter im Drittland transferiert. Der EDSA betont, dass sich der Verantwortliche nicht „blind" auf einen solchen von seinem Auftragsverarbeiter durchgeführten TIA verlassen kann, sondern – je nach Grad des Risikos – unter Umständen verpflichtet sein kann, zumindest die Plausibilität des TIA selbst zu prüfen. Im Ergebnis unterscheidet sich der geforderte Umfang der Kontrollpflichten je nach rechtlicher Grundlage, auf die die Drittlandsübermittlung gestützt wird.

Insgesamt bietet die Stellungnahme des EDSA wichtige Klarstellungen zu Fragen der Praxis. Die Aussagen des EDSA sind letztlich nicht überraschend, sondern im Gesetz selbst angelegt. Der Verantwortliche kann seiner gesetzlich festgelegten Verantwortlichkeit für die Datenschutzkonformität aller Verarbeitungen, die in seinem Auftrag durchgeführt werden, letztlich nicht entgehen, auch nicht bei mehrgliedrigen Auftragsketten mit einer u. U. hohen Anzahl an Auftrags- und Unterauftragsverarbeitern. Lediglich der Umfang und der Detailgrad dessen, was der Verantwortlichen selbst prüfen muss, kann in Abhängigkeit vom Risiko der Verarbeitung variieren. Da der Verantwortliche jedoch aufgrund seiner Rechenschaftspflicht stets in der Lage sein muss nachzuweisen, dass er letztlich auch die Garantien der Unterauftragsverarbeiter hinreichend geprüft hat, wäre er schlecht beraten, wenn er sich stets und unterschiedslos allein auf die von seinen „ersten" Auftragsverarbeiter durchgeführten Prüfung der Garantien der Unterauftragsverarbeiter verlässt; je höher das Risiko der Verarbeitung, umso genauer muss der Verantwortliche auch selbst ggf. etwaige Dokumentationen zu den Unterauftragsverarbeitern

hinterfragen, die ihm von den jeweils übergeordneten Auftragsverarbeitern vorgelegt werden.

4.3 Ein Briefkasten ist keine datenschutzrechtliche Niederlassung

Die Eintragung in einem Handelsregister und Unterhaltung eines Briefkastens stellen noch keine „Niederlassung" im datenschutzrechtlichen Sinne dar.

Anlässlich einer Beschwerde sind wir an das Betreiberunternehmen (nachfolgend: „A") eines Online-Portals herangetreten, das soweit ersichtlich weitestgehend auf den deutschen Markt ausgerichtet ist. Das Unternehmen A gibt auf dem Portal eine Geschäftsadresse auf Zypern und eine Eintragung im zypriotischen Handelsregister an. Unter Berufung hierauf erklärte der Geschäftsführer, er sehe unser Haus nicht als örtlich zuständige Datenschutzaufsichtsbehörde an, zuständig sei aus seiner Sicht vielmehr die zypriotische Aufsichtsbehörde. Wir haben dies angezweifelt, da auf dem Onlineportal für einen bestimmten Teil der dort angebotenen Leistungen das Unternehmen A, für einen anderen Teil der Leistungen hingegen ein davon zu unterscheidendes Unternehmen (nachfolgend: „B") als Verantwortlicher angegeben wird, das in Bayern im Handelsregister eingetragen ist. Der Geschäftsführer beider Unternehmen ist identisch. Als Geschäftsadresse von B wird auf dem Onlineportal und im Handelsregister eine Adresse in Bayern angegeben. Für A wird diese bayerische Adresse zwar an keiner Stelle als Geschäftsadresse angegeben, dennoch bestanden bei dieser Sachlage aus unserer Sicht Anhaltspunkte dafür, dass die Tätigkeit beider Unternehmen – A und B – aus denselben Räumen in Bayern ausgeübt wird, nämlich in der Privatwohnung des Geschäftsführers, die als Geschäftsadresse von B angegeben wird.

Wir haben daher den Geschäftsführer gefragt, an welchem Ort bzw. welchen Orten das Unternehmen A über Niederlassungen verfügt. Dies deshalb, weil die örtliche datenschutzaufsichtliche Zuständigkeit vornehmlich an dem Ort der Niederlassung des Verantwortlichen anknüpft; soweit es sich um eine grenzüberschreitende Verarbeitung im Sinne von Artikel 4 Nr. 23 DS-GVO handelt und die Entscheidungen über die Zwecke und Mittel der Verarbeitung in einer Niederlassung innerhalb der EU bzw. des EWR getroffen werden, sind die Aufsichtsbehörden mehrerer EU- bzw. EWR-Mitgliedstaaten im Rahmen des Kooperationsverfahrens nach dem Kapitel VII der DS-GVO gemeinsam zuständig, wobei es dann unter ihnen gemäß Art. 56 Abs. 1 DS-GVO eine federführende Aufsichtsbehörde gibt.

Vorrangig war damit zu klären, wo genau und in welchen Mitgliedstaaten das Unternehmen A über Niederlassungen verfügt. Eine „Niederlassung" setzt gemäß Erwägungsgrund 22 der DS-GVO eine feste Einrichtung voraus, von der aus effektiv und tatsächlich eine Tätigkeit ausgeübt wird. Maßgeblich für den Niederlassungsbegriff ist somit der Ort, an dem diejenigen geschäftlichen Aktivitäten ausgeübt werden, die einem Unternehmen das Gepräge geben, etwa die wesentlichen Management-Entscheidungen getroffen, Kundenbestellungen bearbeitet, Waren ausgeliefert, Marketing-, Buchhaltungs-, Personalverwaltungs- und sonstige unternehmenstypische Aufgaben tatsächlich wahrgenommen werden. Das bloße Vorhalten eines Briefkastens, in dem die Geschäftskorrespondenz (lediglich) entgegengenommen und abgeholt wird, gehört für sich gesehen nicht zu den Tätigkeiten, die die „effektive und tatsächliche" Ausübung der Unternehmenstätigkeit ausmachen, da es noch nichts darüber aussagt, wo die betreffende (Geschäfts-)Korrespondenz bearbeitet wird und somit die maßgeblichen Unternehmensfunktionen wahrgenommen werden. Auch die Eintragung in einem Handels- oder vergleichbaren Register stellt als solche keine Niederlassung dar, da es sich hierbei nur um eine rechtliche Kategorie

handelt, die noch nichts darüber besagt, wo die für ein Unternehmen wesentlichen Aufgaben tatsächlich wahrgenommen werden. In der Regel sind unter einer Niederlassung vielmehr die Räumlichkeiten zu verstehen, in denen die für ein Unternehmen wesentlichen Aufgaben tatsächlich erfüllt werden, im Rahmen derer die relevante Datenverarbeitung durchgeführt wird. Hierbei ist unerheblich, ob der Verantwortliche selbst Eigentümer oder Mieter dieser Räume ist; maßgeblich ist allein, in welchen Räumen der Verantwortliche die (Geschäfts-)Tätigkeit ausübt, im Rahmen derer die Daten verarbeitet werden. Gerade bei kleinen und Kleinstunternehmen ist es nicht ungewöhnlich, dass die Geschäftstätigkeit in der Privatwohnung einer der am Unternehmen beteiligten Personen (ggf. des einzigen Inhabers des Unternehmens) ausgeübt wird.

Wir haben den Geschäftsführer daher aufgefordert, Belege dafür vorzulegen, dass Unternehmen A in Zypern über die bloße Geschäftsadresse und den Registereintrag auch über Räume verfügt, von denen aus es seine Geschäftstätigkeit ausübt. Derartige Belege wurden trotz mehrfacher Nachfrage bis zum Redaktionsschluss nicht vorgelegt. Die Ermittlungen sind bislang noch nicht abgeschlossen. Sollten sich die Anhaltspunkte bestätigen, dass die Geschäftstätigkeit von A in den Räumen in Bayern ausgeübt wird, stünde es fest, dass unser Haus für die Bearbeitung der Beschwerde örtlich zuständig ist. Gegebenenfalls wäre noch zu prüfen, ob es weitere Niederlassungen (ggf. in anderen Mitgliedstaaten) gibt, in denen das Unternehmen A seine Tätigkeit ausübt; in diesem Fall könnte ggf. das Kooperationsverfahren unter Beteiligung der Aufsichtsbehörden mehrere Mitgliedstaaten zur Anwendung kommen.

4.4 Räumlicher Anwendungsbereich

E-Mail-Kommunikation eines Insolvenzverwalters aus den USA an einzelne in der EU befindliche Gläubiger eines insolventen US-Unternehmens unterfällt nicht pauschal der DS-GVO.

Ein in Deutschland lebender Kunde eines insolventen US-amerikanischen Finanzdienstleisters wandte sich mit einer Beschwerde an uns, die gegen den Insolvenzverwalter des Finanzdienstleisters gerichtet war. Als Insolvenzverwalter war von dem zuständigen US-Gericht eine US-amerikanische Unternehmensberatung bestellt worden. Der Insolvenzverwalter informierte den Kunden – wie auch andere Gläubiger des insolventen Unternehmens – regelmäßig per E-Mail über den Stand des Insolvenzverfahrens. Der deutsche Kunde wünschte, keine E-Mails zu erhalten, was aber seitens des Insolvenzverwalters nicht umgesetzt worden war und zur Beschwerde bei uns führte.

Nach unserer Bewertung unterfiel die Versendung der E-Mails, die Gegenstand der Beschwerde war, jedoch nicht dem räumlichen Anwendungsbereich der DS-GVO. Die Eröffnung des Anwendungsbereichs der DS-GVO nach Art. 3 Abs. 1 erfordert eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer EU-Niederlassung des Verantwortlichen erfolgt. Zwar existieren einige Unternehmen mit Sitz in der Europäischen Union, die zu derselben Unternehmensgruppe wie das als Insolvenzverwalter tätige US-Beratungsunternehmen gehören und somit zumindest grundsätzlich als EU-Niederlassungen des Verantwortlichen in Betracht kämen; jedoch wurde das Insolvenzverfahren nach unseren Erkenntnissen alleine durch Mitarbeiter des US-amerikanischen Beratungsunternehmens betreut. Auch gab es keine Anhaltspunkte dafür, dass die EU-Niederlassungen - ggf. auch nur mittelbar oder mit unterstützenden Tätigkeiten – generell an der Führung von Insolvenzverfahren in den USA beteiligt sind. Damit erfolgte die Verarbeitung personenbezogener Daten, die Gegenstand der Beschwerde war, nicht „im Rahmen der Tätigkeiten" einer EU-Niederlassung des Verantwortli-

chen, so dass der räumliche Anwendungsbereich der DS-GVO nach Art. 3 Abs. 1 nicht eröffnet war. Die DS-GVO war darüber hinaus nach unserer Bewertung auch nicht aufgrund des sog. Marktortprinzips nach Art. 3 Abs. 2 Buchstabe a) räumlich anwendbar. Diese Regelung setzt voraus, dass die Verarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an Personen steht, die sich in der Europäischen Union befinden. Es ist schon fraglich, ob das Führen eines Insolvenzverfahrens in den USA über das Vermögen eines US-amerikanischen Finanzdienstleisters durch den Insolvenzverwalter als „Anbieten von Waren oder Dienstleistungen" an die einzelnen Gläubiger des insolventen Unternehmens angesehen werden kann. Selbst jedoch wenn man letzteres anders sehen wollte, so kann jedenfalls nicht gesagt werden, dass es sich bei der Führung eines Insolvenzverfahrens in den USA um eine Dienstleistung handelt, die der US-amerikanische Insolvenzverwalter „offensichtlich" gerade auch an Personen in der Europäischen Union anzubieten beabsichtigt, wie es Art. 3 Abs. 2 Buchstabe a) DS-GVO voraussetzt (vgl. Erwägungsgrund 23 zur DS-GVO). Dass sich einzelne Gläubiger des insolventen US-Finanzdienstleisters möglicherweise – wie der Beschwerdeführer - in der Europäischen Union aufhalten, reicht für sich gesehen nicht aus um annehmen zu können, dass die Führung des Insolvenzverfahrens oder Teile hiervon, wie etwa die Versendung von E-Mails mit Informationen über den Verfahrensstand ein „offensichtliches" Anbieten an Personen in der EU darstellt; vielmehr sind einzelne Gläubiger, die sich in der EU aufhalten, in diesem Fall lediglich in gleicher Weise von der Dienstleistung betroffen wie alle anderen Gläubiger, sodass es an einer gezielten Ausrichtung der Dienstleistung auf Personen in der EU fehlt.

Im Ergebnis unterfiel die Versendung der E-Mails im vorliegenden Fall somit nicht der DS-GVO, so dass die auf die DS-GVO gestützte Beschwerde des deutschen Kunden nicht erfolgreich war.

4.5 Verzicht auf einen Auskunftsanspruch Art. 15 DS-GVO

Die vergleichsweise Einigung über einen bereits geltend gemachten datenschutzrechtlichen Auskunftsanspruch ist möglich. Dies hat zur Folge, dass der Anspruch auf Auskunft erlischt.

Im Berichtszeitraum wurde über eines unserer Verfahren zum Auskunftsrecht im Beschäftigtenkontext durch das Bayerische Verwaltungsgericht Ansbach entschieden, dass eine vergleichsweise Einigung über einen datenschutzrechtlichen Anspruch möglich ist (vgl. VG Ansbach, U. v. 03.05.2024 – AN K 21.00653).

Der rechtskräftigen Entscheidung lag ein Beschwerdeverfahren beim BayLDA zu Grunde, mit welchem eine nicht erteilte Auskunft eines Arbeitgebers gerügt wurde. Noch vor Erhebung der Beschwerde wurde jedoch ein außergerichtlicher Vergleich geschlossen. Die vom beschwerdeführenden Arbeitnehmer bevollmächtigte Rechtsanwältin erklärte das Einverständnis mit dem – bis zu diesem Zeitpunkt im Streit stehenden - Arbeitszeugnis und teilte mit, dass im Gegenzug selbstverständlich alle anderen Ansprüche erledigt sind. Dies umfasste nach unserem Verständnis auch das Auskunftsersuchen, weshalb wir dem Beschwerdeführer mit einer Abschlussmitteilung daraufhin mitgeteilt haben, dass das Auskunftsersuchen ebenso wie das Beschwerdeverfahren als erledigt angesehen wird. Hiergegen erhob der Beschwerdeführer Klage beim Bayerischen Verwaltungsgericht Ansbach und beantragte das Landesamt für Datenschutzaufsicht zu verurteilen, gegen den Beschwerdegegner eine Abhilfemaßnahme gem. Art. 58 Abs. 2 DS-GVO zu ergreifen.

Auch das Bayerische Verwaltungsgericht Ansbach sah den noch vor dem Vergleich geltend gemachten Auskunftsanspruch als erloschen an. Die Erklärung der Rechtsanwältin war gemäß

§§ 133,157 BGB nach dem objektiven Empfängerhorizont auszulegen. Die Bewertung des Bayerische Landesamtes für Datenschutzaufsicht, dass damit alles, was zuvor zwischen dem Kläger und dem Beschwerdegegner thematisiert wurde, erledigt ist, war aus Sicht des Gerichts nicht zu beanstanden. Das Gericht sah weder in der DS-GVO noch in anderen Rechtsvorschriften einen Anhaltspunkt dafür, dass über einen datenschutzrechtlichen Anspruch keine vergleichsweise Einigung möglich wäre.

Jedenfalls auf eine bereits geltend gemachte Auskunft kann somit insbesondere durch einen arbeitsrechtlichen Vergleich verzichtet werden – selbst, wenn nicht explizit auf das Auskunftsrecht Bezug genommen wird, sich aus dem Gesamtkontext jedoch ergibt, dass dieser ebenfalls von der Einigung mitumfasst sein soll.

4.6 Europaweite Prüfung zur Umsetzung des Auskunftsrechts (CEF 2024)

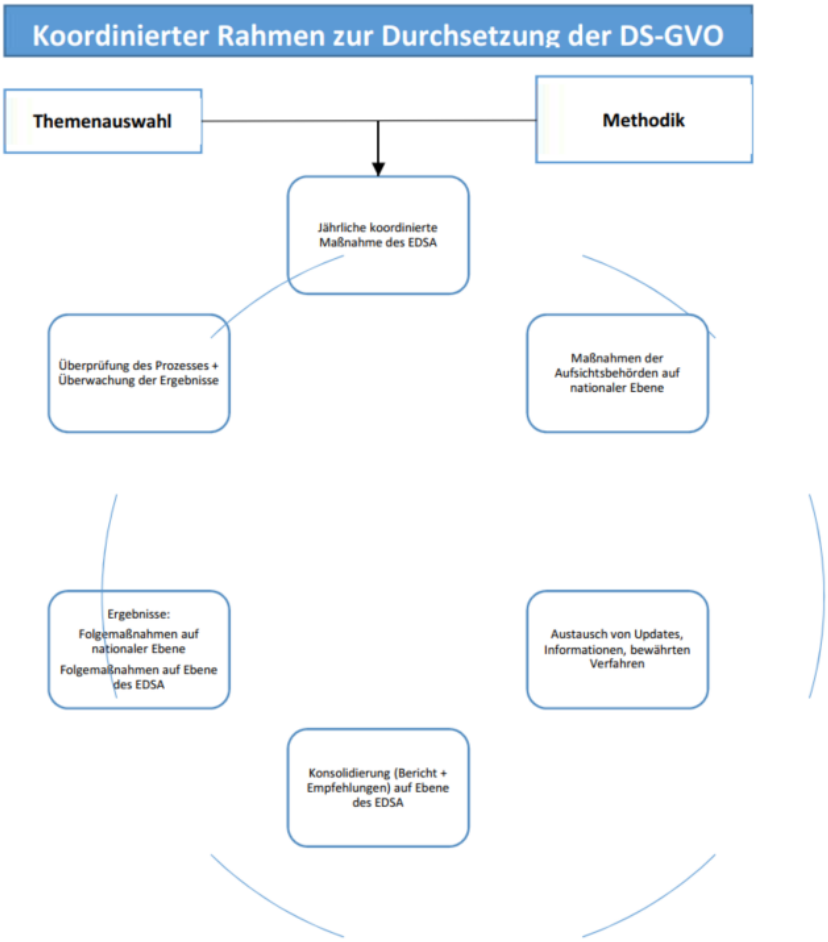
Durch die Beteiligung an der europaweiten Prüfung zur Umsetzung des Auskunftsrechts konnten wir Einblicke in den Umsetzungsstand in Bayern, Deutschland und in der Europäischen Union gewinnen. In der Folge und unter Heranziehung der Erkenntnisse aus unserer Bearbeitungspraxis ist es uns möglich, Verantwortliche zielgerichtet zu sensibilisieren und Handlungsempfehlungen zu geben.

„Verfügen Sie über einen definierten Prozess zur Bearbeitung von Auskunftsanträgen nach Art. 15 DS-GVO?“, „Welche Maßnahmen ergreifen Sie, um sicherzustellen, dass Auskunftsanträge nach Art. 15 DS-GVO unverzüglich, in jedem Fall jedoch innerhalb eines Monats nach Eingang beantwortet werden?“, „Wie ermitteln Sie, welche Daten Sie im Rahmen eines Auskunftsantrags nach Art. 15 DS-GVO für die Beauskunftung berücksichtigen müssen?“ , „Unter welchen Umständen bitten Sie die betroffene Person, ihren Auskunftsantrag nach Art. 15 DS-GVO zu präzisieren?“ – das sind nur einige der Fragen, zu deren Beantwortung wir ausgewählte Verantwortliche im Rahmen der europaweiten Aktion zur koordinierten Durchsetzung der DS-GVO („Coordinated Enforcement Framework (CEF)“) für 2024 aufgefordert haben.

Was ist der CEF?

Der CEF bietet eine Struktur für die Koordinierung jährlich wiederkehrender Prüfungen der europäischen Datenschutz-Aufsichtsbehörden, deren Gegenstand jeweils vom Europäischen Datenschutzausschuss (EDSA) festgelegt wird, wobei die Teilnahme nicht verpflichtend ist. Mit dem CEF sollen auf flexible, aber koordinierte Weise gemeinsame Maßnahmen im weiteren Sinne unterstützt werden, die von der gemeinsamen Sensibilisierung und Informationsbeschaffung bis hin zu Durchsetzungsmaßnahmen und gemeinsamen Untersuchungen reichen. Die Durchführung der Prüfaktion selbst und daran anschließender Folgemaßnahmen ist Aufgabe der teilnehmenden Datenschutzbehörden in ihrem jeweiligen nationalen Zuständigkeitsbereich (Art. 55 Abs. 1 DS-GVO). Die Ergebnisse der jeweiligen Prüfaktion werden im Ausschuss in einem europäischen Bericht mit Empfehlungen für die Nachbereitung der jährlichen Maßnahme (z. B. Folgemaßnahmen zur Durchsetzung auf nationaler Ebene oder Leitlinien auf Ebene des EDSA) zusammengefasst. Die Initiierung und Koordination der Prüfaktionen erfolgt auf Grundlage der Aufgabe des EDSA, eine einheitliche Anwendung der DS-GVO, insbesondere durch die Förderung der Zusammenarbeit zwischen den Aufsichtsbehörden sicherzustellen (Art. 70 Abs. 1 S. 1, S. 2 Buchstabe u) DS-GVO).

Der CEF-Lebenszyklus, der unter anderem die jährlich koordinierte Maßnahme umfasst, wird in dem EDSA-Dokument über den Rahmen für eine koordinierte Durchsetzung der Verordnung 2016/679 , dort S. 8 wie folgt veranschaulicht:



Wer wurde geprüft?

Wir haben insgesamt 20 Verantwortliche, mit einem auf europäischer Ebene abgestimmten Fragenkatalog, angeschrieben und zur Stellungnahme aufgefordert. Ziel war die Überprüfung vorhandener Prozesse, daher wählten wir für die Prüfung Verantwortliche aus verschiedenen Branchen aus, bei denen wir davon ausgegangen sind, dass dort jährlich eine größere Anzahl an Beschwerden eingeht. Umso mehr überraschte es, dass im abgefragten Zeitraum, d. h. im Jahr 2023 bei mehr als der Hälfte der Verantwortlichen unter 50 Auskunftsanträge gem. Art. 15 DS-GVO eingingen. Dieses Ergebnis wurde europaweit sogar noch unterboten, da insgesamt rund 74% der antwortenden Verantwortlichen angaben, im Jahr 2023 nur null bis zehn Auskunftsanträge erhalten zu haben.

Insgesamt haben 1.185 Verantwortliche im gesamten EWR (davon 116 Verantwortlicher in Deutschland) den Fragebogen beantwortet, wobei der private und der öffentliche Sektor gleichermaßen vertreten war.

Was wurde festgestellt?

Auch wenn die „bayerischen" Vorgänge im Berichtszeitraum noch nicht vollständig zum Abschluss gebracht wurden, konnten wir aus den uns vorliegenden Stellungnahmen bereits erkennen, welche Anforderungen bei den geprüften Verantwortlichen gut umgesetzt sind und in welchen Bereichen es Sensibilisierungsbedarf gibt und eine Nachbesserung der Prozesse zu veranlassen ist.

Diese Erkenntnisse wurden auch im Austausch mit den anderen teilnehmenden Behörden auf nationaler und europäischer Ebene bestätigt – neben unserer Behörde haben sich in Deutschland die Landesaufsichtsbehörden Brandenburg, Mecklenburg- Vorpommern, Niedersachsen, Rheinland-Pfalz, dem Saarland und Schleswig-Holstein sowie die BfDI an der Prüfaktion beteiligt sowie weitere 22 europäische Datenschutzaufsichtsbehörden.

Entsprechend der Vorgaben aus dem CEF wurden alle nationalen Feststellungen auf der Ebene des EDSA in einem Bericht konsolidiert und Empfehlungen für die Nachbereitung der jährlichen Maßnahmen abgegeben. Der Bericht enthält die nationalen Berichte im Anhang, wobei sich die teilnehmenden deutschen Aufsichtsbehörden darüber verständigt haben, einen gemeinsamen deutschen Bericht zu verfassen.

Insgesamt konnte positiv festgestellt werden, dass bei den von uns geprüften Verantwortlichen die Leitlinien zum Auskunftsrecht bekannt waren und größtenteils für die Beantwortung von Auskunftsersuchen herangezogen wurden bzw. künftig herangezogen werden und ein Prozess zur Bearbeitung von Auskunftsersuchen vorhanden ist. Nachbesserungsbedarf wurde insbesondere hinsichtlich der Vollständigkeit der Auskunft, der Identifizierung und Authentifizierung sowie der Dauer der Aufbewahrung von Auskünften mitsamt Kommunikationsverlauf erkannt.

Im Einzelnen:

Auch wenn die **Prozessbeschreibung** und – gestaltung in die Organisationshoheit der Verantwortlichen fällt, sollten diese ein strukturiertes Verfahren zur Bearbeitung von Auskunftsanträgen vorhalten, sodass beim Eingang von Auskunftsersuchen, diese unverzüglich und ordnungsgemäß bearbeitet werden können. Die uns vorgelegten Prozessbeschreibungen ließen erkennen, dass gerade in größeren Unternehmen eine zentrale Bearbeitung von Auskunftsersuchen in einer vom Tagesgeschäft losgelösten Organisationseinheit zielführend und effektiv sein kann. Dies kann beispielsweise unter Nutzung einer speziellen Software erfolgen, die die Informationen zu der betroffenen Person aus den verschiedenen Fachbereichen/Organisationseinheiten und ihren jeweiligen Systemen zusammenträgt, zu einer Auskunft zusammenführt, diese mit eingeschränkt verarbeiteten Daten ergänzt, die Vollständigkeit überprüft und diese der betroffenen Person zur Verfügung stellt.

Der Einsatz von entsprechenden Softwarelösungen hat sich darüber hinaus auch zur Erkennung von Auskunftsersuchen, die beispielsweise nicht über die hierfür vorgesehenen Kanäle eingehen oder auch für die Fristenkontrolle, als praktisches Hilfsmittel erwiesen (vgl. hierzu auch EDSA-Bericht, Kapitel 4.2.3, S. 18; DE-Bericht in der Anlage zum EDSA-Bericht, S. 61 ff.).

Auffällig häufig erreichte uns und auch andere an der Prüfung teilnehmende Aufsichtsbehörden die Antwort, dass **formale Anforderungen** an ein Auskunftsersuchen gestellt werden (vgl. hierzu auch EDSA-Bericht, Kapitel 4.2.4, S. 20; DE-Bericht in der Anlage zum EDSA-Bericht, S. 63 f.). Zum Teil wurden Auskunftsersuchen von Verantwortlichen nur dann akzeptiert und als Auslöser für die Frist gem. Art. 12 Abs. 3 S. 1 DS-GVO angesehen, wenn diese schriftlich oder in Textform gestellt wurden. Mündliche Anträge wurden oftmals nicht akzeptiert. Dabei wurde

insbesondere die fehlende Möglichkeit zur Authentifizierung der betroffenen Personen angeführt. Dass eine solche durch gezielte Abfragen jedoch möglich ist, zeigten hingegen andere von uns geprüfte Verantwortliche in Ihren Prozessen auf. Diese fragten z. B. verschiedene Informationen ab, um sicherzustellen, dass es sich bei der auskunftsersuchenden Person tatsächlich um die betroffene Person handelt.

Zudem wurde in einigen Fällen angeführt, dass Auskunftsersuchen nur dann akzeptiert und bearbeitet würden, wenn ein bestimmter, vom Verantwortlichen vorgegebener Kommunikationskanal genutzt wird.

Dem widerspricht der EDSA jedoch bereits in seinen Leitlinien 01/2022 zum Auskunftsrecht. Hierin wird einerseits ausgeführt, dass die DS-GVO keine Anforderungen an die Form des Antrags auf Auskunft gem. Art. 15 DS-GVO stellt (Rn. 52). Andererseits wird hierin darauf hingewiesen, dass selbst dann, wenn ein Kommunikationskanal seitens des Verantwortlichen festgelegt wurde, auch Auskunftsanträge zu bearbeiten sind, die nicht über diesen beim Verantwortlichen eingingen (Rn. 138).

Sowohl im Rahmen der koordinierten Prüfung, als auch bei unseren tagtäglichen Eingängen zum Auskunftsrecht gem. Art. 15 DS-GVO stellen wir fest, dass (weiterhin) einige Verantwortliche davon ausgehen, dass die Beantwortung von Auskunftsersuchen generell in einem **zweistufigen Verfahren** erfolgen kann (vgl. hierzu auch EDSA-Bericht, Kapitel 4.2.6, S. 24; DE-Bericht in der Anlage zum EDSA-Bericht S. 68 f.). Auf der ersten Stufe werden standardisierte/rudimentäre Auskünfte gegeben und erst auf weitere Nachfrage der betroffenen Person, in einer zweiten Stufe konkrete Informationen zu der betroffenen Person erteilt. Dies kann jedoch dazu führen, dass die betroffene Person nicht die vollständige Auskunft erhält und ihr Informationen verborgen bleiben. Dies kann insbesondere dann der Fall sein, wenn der betroffenen Person die einzelnen Verarbeitungsvorgänge, Datenbanken u. ä. nicht bekannt sind. Auch wenn eine entsprechende zweistufige Vorgehensweise in der Vergangenheit teilweise auch von den Aufsichtsbehörden vertreten wurde, ist bereits seit einigen Jahren klargestellt, dass eine Auskunft – soweit der Auskunftsantrag selbst nicht eine Einschränkung beinhaltet – grundsätzlich von Anfang vollständig zu erteilen ist. Eine Ausnahme kann nur dann bestehen, wenn große Mengen personenbezogener Daten verarbeitet werden. In diesem Fall kann der Verantwortliche eine Präzisierung dahingehend, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, verlangen (vgl. Erwägungsgrund 63 S.7 DS-GVO). Die Leitlinien zum Auskunftsrecht (Rn. 35 b) sehen es als Voraussetzung an, dass der Verantwortliche bei dem konkreten Ersuchen Zweifel daran haben muss, ob das Auskunftsersuchen wirklich darauf abzielt, Informationen über jegliche Datenverarbeitung in allen Tätigkeitsbereichen zu erhalten. Soweit ein Verantwortlicher die betroffene Person zur Präzisierung auffordert, müssen der betroffenen Person aussagekräftige Informationen über die Verarbeitungsvorgänge bereitgestellt werden (vgl. Erleichterung der Antragstellung, Art. 12 Abs. 2 DS-GVO). Nur so ist es der betroffenen Person möglich, Kenntnis von diesen zu erlangen und ihr Auskunftsersuchen zu begrenzen, soweit sie dies wünscht. Bestätigt die betroffene Person dennoch, dass sie eine vollständige Auskunft wünscht, muss ihr auch die vollständige Auskunft zur Verfügung gestellt werden.

Damit die Bitte des Verantwortlichen nach Präzisierung durch die betroffene Person zulässig ist, bedarf es im konkreten Einzelfall nachweisbar

- einer großen Menge an Informationen und
- konkreter Zweifel daran, dass nicht eine vollumfängliche Auskunft, son-

dern ggf. nur für bestimmte Verarbeitungsvorgänge eine Teilauskunft verlangt wird

- einer Information der betroffenen Person über die sie betreffenden Verarbeitungstätigkeiten.

Soweit diese Voraussetzungen erfüllt sind, kann der Verantwortliche zur Präzisierung i. S. d. ErwGr. 63 S. 7 DS-GVO auffordern, was zur Folge hat, dass der Verantwortliche eine Antwort der betroffenen Person abwarten kann, bevor er ihr weitere Informationen entsprechend des Antrags zur Verfügung stellt.

Klarstellend erwähnt wird seitens des EDSA nochmals, dass auch ein mehrstufiger Ansatz („layered approach"), wie ihn die Leitlinien zur Transparenz, Rn. 35 ff. in Bezug auf Datenschutzhinweise empfehlen, nicht dazu führt, dass die Auskunft eingeschränkt werden kann bzw. die Auskunft in mehreren (Antrags-)Schritten erteilt wird. Vielmehr handelt es sich hierbei um eine Möglichkeit, eine umfangreiche Auskunft leicht verständlich zur Verfügung zu stellen (vgl. Art. 12 Abs. 1 DS-GVO). Der Ansatz ist geeignet, wenn es aufgrund der großen Anzahl personenbezogener Daten für die betroffene Person schwierig wäre, die Informationen ohne, dass eine Abschichtungen vorgenommen wurde, zu verstehen. In diesem Fall kann die Information auf mehreren Ebenen bereitgestellt werden. In Kenntnis hiervon kann die betroffene Person dann selbst auswählen, welche Ebenen sie aktiv einsieht. Für den Zugang auf Unterebenen darf jedoch kein weiterer Antrag der betroffenen Person erforderlich sein und es darf auch keinen unverhältnismäßigen Aufwand für diese bedeuten. Kurz gesagt: es müssen alle Ebenen gleichzeitig zur Verfügung bzw. zum Abruf bereitgestellt werden, so dass die betroffene Person selbst und ohne, dass sie einen weiteren Antrag stellen muss, auswählen kann, welche Informationen sie ggf. in welcher Reihenfolge oder Tiefe zur Kenntnis nimmt. Dieser Ansatz ist deshalb grundsätzlich primär für den Online-Bereich geeignet.

Eine weitere Feststellung, die wir bei der Auswertung machen konnten, ist das vielfach noch immer ein ausdrücklicher Antrag gem. Art. 15 Abs. 3 DS-GVO gefordert wird, damit Dokumentenauszüge bzw. Auszüge aus Datenbanken zur Verfügung gestellt werden. Ein solcher (weiterer) Antrag darf jedoch nicht verlangt werden, vielmehr besteht eine Verpflichtung zur Bereitstellung der Kopie der personenbezogenen Daten (Reproduktionen von Dokumenten/Auszüge aus Datenbanken nur soweit für die Verständlichkeit der Auskunft erforderlich, vgl. hierzu unseren 12. Tätigkeitsbericht, Kapitel 4.4), die Gegenstand der Verarbeitung sind, so dass die betroffene Person die Rechtmäßigkeit der Verarbeitung verstehen und überprüfen kann.

Dies betonen auch die Leitlinien zum Auskunftsrecht aus dem Jahr 2022 (Rn. 23), als auch die EuGH-Entscheidungen vom 4.5.2023, Rs. C-487/21 und vom 26.10.2023, C-307/22 die Ausführungen zu Art. 15 Abs. 3 DS-GVO enthalten (**Kopie der personenbezogenen Daten**). Diese stellen fest, dass es sich hierbei um eine Modalität der Auskunftserteilung handelt, anstatt, wie von einer überwiegenden Anzahl der geprüften Verantwortlichen angenommen um ein eigenes Recht auf Kopie (vgl. hierzu auch EDSA-Bericht, Kapitel 4.2.1, S. 15 f.)

Auch unsere Erfahrungen aus der Beschwerdebearbeitung hinsichtlich der **Identifizierung und Authentifizierung bei Auskunftsersuchen** spiegelten sich in den Rückmeldungen wieder. Es werden regelmäßig - vermutlich pauschal -Zusatzinformationen oder gar die Zusendung von Kopien von Identitätsausweisen gefordert (vgl. hierzu EDSA-Bericht 4.2.4, S. 20 ff.; DE-Bericht in der Anlage zum EDSA-Bericht, S. 64 f.). Dies widerspricht jedoch dem Grundsatz der Datenminimierung sowie den Regelungen des Art. 12 Abs. 2 sowie Abs. 6 DS-GVO.

Identifizierung bedeutet, dass der Verantwortliche die Informationen, die sich auf die antragstellende Person beziehen, dieser auch zuord-

nen kann. Hierfür sollte der Verantwortliche zunächst die von der betroffenen Person im Rahmen des Auskunftsersuchens angegebenen Daten mit den bei ihm vorhandenen Daten abgleichen, z. B. können regelmäßig über den Namen oder über eine Kundennummer die zu einer betroffenen Person gespeicherten Informationen identifiziert werden. Ist eine Zuordnung anhand der von der auskunftsersuchenden Person zur Verfügung gestellten Daten nicht möglich, z. B. weil es sich um pseudonymisierte Daten, die nur einer Kennung zugeordnet werden können, handelt, können zusätzliche Daten (bspw. eine Kennung) zu Zwecken der Identifizierung verlangt werden (Art. 12 Abs. 2 i. V. m. Art. 11 Abs. 2 DS-GVO). Hierzu muss der Verantwortliche die betroffene Person darüber informieren, dass er nicht in der Lage ist, diese zu identifizieren. Stellt die betroffene Person daraufhin (ausreichende) zusätzliche Informationen zur Verfügung, ist dem Auskunftsersuchen nachzukommen. Andernfalls kann der Verantwortliche die Beauskunftung verweigern.

Davon zu unterscheiden ist der Fall, wenn „begründete Zweifel an der Identität" bestehen, d. h. Zweifel bestehen, dass es sich bei der auskunftsersuchenden Person tatsächlich um die betroffene Person handelt, über deren Daten Auskunft verlangt wird. In diesem Fall dürfen und müssen Verantwortliche „zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind" (Art. 12 Abs. 6 DS-GVO). Das können weitere (verhältnismäßige) Authentifizierungsangaben sein, beispielsweise können weitere, mit dem vorhandenen Datensatz abgleichbare Angaben erfragt werden, die in der Kumulation nur die betroffene Person selbst kennen kann.

Pauschal die Kopie eines Ausweisdokuments zu verlangen ist jedoch nicht zulässig. Im Regelfall ist eine Kopie weder geeignet noch erforderlich, um eine Authentifizierung durchzuführen. Darüber bestehen Missbrauchsrisiken, soweit die Personalausweiskopie missbräuchlich durch unberechtigte Personen genutzt werden.

Ist im Einzelfall die Authentifizierung mittels Ausweis gerechtfertigt, so muss diese in der Art und Weise erfolgen, dass keine weiteren Risiken für die betroffene Person geschaffen werden und die entsprechende Verarbeitung den Grundsätzen der DS-GVO gerecht wird (insbesondere Grundsatz der Datenminimierung sowie der Integrität und Vertraulichkeit). Hierzu kann beispielsweise ein Post-Ident-Verfahren, bei dem der Postbote sich vor Übergabe des Briefes den Personalausweis vorlegen lässt bzw. die Nutzung der Online-Funktion des Personalausweises eine praktikable Lösung bieten – einer Ausweiskopie bedarf es dann nicht.

Die Prüfung offenbarte darüber hinaus, dass die erteilten Auskünfte, sowie die zugehörige Kommunikation zwischen der betroffenen Person und dem Verantwortlichen unterschiedlich lange **aufbewahrt** werden, wobei eine Differenzierung zwischen einer Negativauskunft und einer Auskunft häufig nicht erfolgte (vgl. hierzu EDSA-Bericht, Kapitel 4.2.2, S. 17 f.; DE-Bericht in der Anlage zum EDSA-Bericht, S. 58).

Als Grund hierfür konnten wir ausmachen, dass zwischen den grundsätzlichen Verpflichtungen Verantwortlicher zur Datenlöschung und der Notwendigkeit, die vollständige Erfüllung von Betroffenenbegehren auf Auskunft im Prüf- oder Streitfall rechtssicher nachweisen zu müssen ein Spannungsverhältnis besteht, für dessen Auflösung keine hinreichenden Lösungsansätze bereit stehen: So erfolgte in einem Fall grundsätzlich keine Speicherung von Auskunftsanträgen, sondern diese werden unmittelbar nach Beantwortung gelöscht, während in anderen Fällen mehrjährige Aufbewahrungsdauern angegeben wurden. Zudem erfolgte teilweise eine Bearbeitung und Speicherung der Auskunft sowie des dazugehörigen Schriftverkehrs im Produktivsystem, so dass mitunter weitreichende Speicher- und auch Zugriffsmöglichkeiten bestanden.

Regelmäßig akzeptieren wir eine Aufbewahrungsdauer, die sich an § 31 Ordnungswidrigkeitengesetz (OWiG) sowie der allgemeinen zivilrechtlichen Verjährungsfrist von 3 Jahren, beginnend mit dem Schluss des Jahres in dem der Anspruch entstanden ist und der Gläubiger von den Anspruch begründenden Umständen und der Person des Schuldners Kenntnis erlangt hat, oder ohne grobe Fahrlässigkeit erlangen hätte müssen, orientiert. In Einzelfällen wurden uns längere Aufbewahrungsfristen benannt, die wir – soweit eine Erforderlichkeit dargelegt wurde – ebenfalls akzeptieren konnten. Auffällig war, dass uns in den wenigsten Fällen eine datenschutzrechtliche Befugnis für die Aufbewahrung benannt wurde.

Welche Empfehlungen gibt es?

Um einen Gesamtüberblick über die Ergebnisse der europaweiten Prüfung zur Umsetzung des Auskunftsrechts auf europäischer sowie auf nationaler Ebene gewinnen zu können, empfehlen wir Ihnen die Lektüre des CEF-Reports. Hieraus ergeben sich nicht nur Empfehlungen, denen die für die Verarbeitung Verantwortlichen Rechnung tragen sollen, sondern es werden auch Empfehlungen an die Aufsichtsbehörden sowie dem EDSA (z. B. Sensibilisierung, Überarbeitung der Leitlinien, Entwicklung spezifischer Leitlinien) selbst formuliert. Denn die Prüfung dient nicht nur dazu, Verantwortliche hinsichtlich der Umsetzung des Auskunftsrechts zu überprüfen, sondern ermöglichte es den teilnehmenden Aufsichtsbehörden einen Überblick über die verschiedenen Umsetzungsmodelle zu erhalten und sich hierzu auszutauschen.

Für uns bestätigt sich im Ergebnis wiederum, dass eine gute Organisation und Struktur bei der Datenverarbeitung dazu beitragen, den Aufwand bei der Beantwortung von Auskunftsersuchen deutlich zu minimieren. Ist beispielsweise aus dem Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO schnell erkennbar, welche Stellen/Einheiten, welche Daten wie verarbeiten kann sich die Person/Stelle, die für eine ordnungsgemäße Beauskunftung bei dem Verantwortlichen zuständig ist, hieran orientieren. Dies kann einerseits viel Zeit ersparen und verhindert zudem, dass er sich im Nachgang mit Beschwerden wegen unvollständig erteilter Auskunft befassen muss. Neben der Empfehlung, bei der Umsetzung des Auskunftsrechts und der Erteilung von Auskünften die Leitlinien zum Auskunftsrecht zu beachten, empfehlen wir Verantwortlichen – nicht nur zum Zwecke der effektiven Bearbeitung von Auskunftsersuchen - für eine strukturierte Datenorganisation und klare Prozesse zu sorgen.

5

Datenschutzbeauftragte

5 Datenschutzbeauftragte

5.1 Aktualität der Kontaktdaten von Datenschutzbeauftragten (DSB)

Die vom Verantwortlichen zu veröffentlichenden DSB-Kontaktdaten sind aktuell zu halten.

Uns lagen im Berichtszeitraum mehrfach Sachverhalte vor, bei welchen eine DSB-Benennung (entweder aufgrund eines Wechsels oder eines Wegfalls der Benennpflicht) geendet bzw. sich geändert hatte, aber der Verantwortliche in seiner Veröffentlichung der DSB-Kontaktdaten nach Art. 37 Abs. 7 DS-GVO, bzw. in seinen Datenschutzinformationen nach Art. 13 / 14 DS-GVO weiterhin die zwischenzeitlich veralteten Kontaktdaten vorhielt; teils sogar über mehrere Jahre.

Sinn und Zweck der Vorschriften zur Information über benannte DSB und zur Veröffentlichung der DSB-Kontaktdaten ist es, den betroffenen Personen insbesondere zu ermöglichen, diese entsprechend Art. 38 Abs. 4 DS-GVO zu Rate ziehen. Dieser gesetzlich vorgesehenen Funktion können die bereitgestellten Angaben nur dann gerecht werden, wenn diese auch korrekt, bzw. auf dem neuesten Stand sind. Inkorrekte / veraltete Angaben stellen daher einen datenschutzrechtlichen Verstoß dar.

Sollten solche nicht mehr den Tatsachen entsprechende Angaben zudem auch personenbezogene Daten bisheriger DSB enthalten, kommt hierzu außerdem noch ein Verstoß gegen die Rechtmäßigkeit deren Verarbeitung / Offenlegung, da spätestens mit Wegfall der DSB-Funktion keine Zulässigkeitsgrundlage mehr besteht, solche Daten weiterhin allgemein einsehbar vorzuhalten.

5.2 Mitglieder der Geschäftsführung als Datenschutzbeauftragte

Die Geschäftsführung eines Verantwortlichen kann nicht gleichzeitig die Funktion dessen DSB wahrnehmen.

Im Berichtszeitraum mussten wir mehrfach feststellen, dass Verantwortliche eine Person als DSB benannt hatten, die gleichzeitig Teil der Geschäftsführung des Verantwortlichen war.

Nach Art. 38 Abs. 6 DS-GVO können DSB zwar andere Aufgaben und Pflichten wahrnehmen, wobei jedoch der Verantwortliche sicherzustellen hat, dass derartige Aufgaben und Pflichten nicht zu einem Interessenskonflikt führen.

Bei der Benennung einer Person der Geschäftsführung als DSB handelt es sich um einen geradezu beispielhaften Fall eines solchen unzulässigen Interessenskonflikts, da damit eine Konstellation geschaffen wird, in welcher Datenschutzbeauftragte sich selbst bei der Bestimmung von Mitteln und Zwecken der Datenverarbeitung überprüfen müssten, während sie maßgeblich den Geschäftsbetrieb des Verantwortlichen und die damit zusammenhängenden Verarbeitungen steuern.

Die Benennung eines Mitglieds der Geschäftsführung ist demnach nach unserer Auffassung im Einklang mit Rechtsprechung des EuGH (Urt. v. 2.2.2023, Rs. C. 453/21) regelmäßig nicht geeignet, einer bestehenden DSB-Benennpflicht nachzukommen.

6

Finanzwirtschaft

6 Finanzwirtschaft

6.1 Berichtigung nach Art. 16 DS-GVO bei aufbewahrungspflichtigen Daten mit Veränderungsverbot

Wenn eine Berichtigung datenschutzrechtlich erforderlich, aber aufgrund entgegenstehender gesetzlicher Aufbewahrungspflichten nicht im Originalbestand möglich ist, kann und muss die Berichtigung in Form einer Hinzuspeicherung erfolgen.

An uns hat sich ein Betroffener gewandt, der kürzlich eine Vertragsleistung seiner Bank gekündigt hatte. Im Nachgang hat er dann Kenntnis davon erhalten, dass die Bank im Rahmen der entsprechenden Formular-Übermittlung an ihren Kartendienstleister fälschlicherweise nicht diese Kündigung, sondern eine Kartensperre wegen Bonitätsverschlechterung als Beendigungsgrund angegeben hatte.

Der Betroffene wandte sich deshalb mit einem Berichtigungsersuchen an die Bank, welches darauf gerichtet war, die fehlerhafte Angabe im entsprechenden Geschäftsdokument durch die korrekte Angabe zu ersetzen. Die Bank verweigerte eine entsprechende Berichtigung jedoch mit Verweis darauf, dass das Geschäftsdokument gesetzlichen Aufbewahrungspflichten und damit auch einem gesetzlichen Veränderungsverbot unterfallen.

Im Rahmen unserer Prüfung der Angelegenheit stellten wir zunächst fest, dass die Bank durch die Verarbeitung der unrichtigen Daten einen Verstoß gegen Art. 5 Abs. 1 Buchstabe d) DS-GVO verwirklicht hatte. Obwohl die Bank zusätzlich vortrug, dass diese unrichtigen Daten keine Auswirkungen auf zukünftige Entscheidungen unter Verwendung der Bonität des Betroffenen haben würden, standen diese Daten einem Berichtigungsersuchen nach Art. 16 DS-GVO auch offen.

Gleichzeitig erwies sich die Auffassung der Bank als plausibel, dass das fragliche Dokument, welches die unrichtigen Daten enthielt, zum Gegenstand gesetzlicher Aufbewahrungspflichten geworden ist, die eine Veränderung der Inhalte verbieten, sodass ein Spannungsfeld entstanden war, in welchem die Bank zwar zur Berichtigung verpflichtet war, aber die geforderte Berichtigung im fraglichen Dokument nicht vornehmen konnte, ohne gegen andere Rechtsvorschriften zu verstoßen.

Mit der Entscheidung, die Berichtigung in dieser Situation vollständig zu verweigern, verwirklichte die Bank jedoch einen Datenschutzverstoß.

In einer Situation wie der vorliegenden, konnte die Bank zwar nachvollziehbar keine Berichtigung im verarbeiteten Dokument selbst vornehmen. Das oben aufgezeigte Spannungsfeld kann jedoch dadurch aufgelöst werden, dass dem Dokument, welches die unrichtigen Daten enthält, ein weiteres Dokument hinzugespeichert wird, welches durch ein Aufzeigen der Unrichtigkeit der Daten im Ursprungsdokument und eine Nennung der berichtigten Daten die Berichtigungsfunktion erfüllt.

Dieser Lösung ist die Bank letztlich auch nachgekommen. Allerdings handelte es sich dabei nicht lediglich um ein freiwilliges Entgegenkommen, sondern die Berichtigung in dieser Form wäre bereits auf das initiale Berichtigungsersuchen hin (statt der Ablehnung) geboten gewesen.

6.2 Herausgabe der Anlegerdaten aus Publikumsgesellschaften an Mitgesellschafter

Der EuGH zeigt die Prüfmaßstäbe für Auskünfte zu Mitgesellschaftern auf.

Eine Fallgestaltung, mit der wir wiederholt zu tun haben ist, dass Beteiligte einer Publikumsgesellschaft mit den ihnen unbekannten Mitbeteiligten Kontakt aufnehmen möchten, z. B. um diesen ein Kaufangebot zu deren Gesellschaftsanteilen zu machen. Zu diesem Zweck fordern sie bei der Gesellschaft entsprechende Daten an (z. B. Namen, Anschriften, Beteiligungshöhe).

Die Fälle die uns beschäftigen, sind dann insbesondere solche, bei welchen diese Daten entweder freiwillig oder aufgrund gerichtlicher Entscheidungen tatsächlich herausgegeben werden und es zu solchen Kontaktaufnahmen kommt.

Bereits in unserem Tätigkeitsbericht 2017 / 2018 hatten wir hierzu die Verarbeitungen der Person betrachtet, von der solche Angebote zum Aufkauf ausgehen, und kamen hierbei, auch unter Bezug auf das Urteil des Bundesgerichtshofs (BGH) vom 05.02.2013 (II ZR 134/11), zu dem Ergebnis, dass sich die Verarbeitungen zu diesem Zweck noch in einem datenschutzrechtlich zulässigen Rahmen bewegen.

Daneben gingen wir in unserer Beratungspraxis bis zum Berichtsjahr auch davon aus, dass ebenso die Herausgabe der Daten durch die Gesellschaft jedenfalls im Rahmen des Art. 6 Abs. 1 UAbs. 1 Buchstabe b) DS-GVO eine datenschutzrechtlich zulässige Verarbeitung darstellt. Hierzu hatte auch der BGH zuletzt nochmals mit Beschluss vom 24.10.2023 (II ZB 3/23) entschieden, dass die betrachtete Gesellschaft ein entsprechendes Auskunftsersuchen zu beauskunften habe und dem das geltende Datenschutzrecht nicht entgegenstehe. Unter anderem wird ausgeführt, dass wer sich an einer Publikumsgesellschaft beteiligt, damit rechnen müsse, dass die eigenen Daten und Beteiligungshöhe an weitere Beteiligte mitgeteilt werden. Der Gesellschaftsvertrag begründe ein unentziehbares mitgliedschaftliches Recht, Kenntnis über die weiteren Beteiligten und deren Beteiligungshöhe zu erhalten. Vertragsklauseln im Gesellschaftsvertrag, die eine solche Herausgabe ausschließen, verwarf der BGH als unwirksam.

Auf eine entsprechende Vorlage durch das Amtsgericht München hin, hat sich nun im Berichtsjahr auch der Europäische Gerichtshof (EuGH) mit dieser Datenherausgabe durch solche Gesellschaften befasst (Urteil EuGH vom 12.09.2024, C-17/22 und C-18/22). Anhand dessen Einschätzung wird das vorlegende Gericht die Thematik nun nochmals näher betrachten müssen.

Zwar führt auch der EuGH aus, dass eine Herausgabe im Rahmen des Art. 6 Abs. 1 UAbs. 1 Buchstabe b) DS-GVO zulässig sein kann, wenn sie objektiv unerlässlich zur Erfüllung des Gesellschaftsvertrags ist, sodass der Hauptzweck des Vertrages andernfalls – also ohne diese Verarbeitung – nicht erfüllt werden könnte. Aus Sicht des EuGH ist dies jedoch jedenfalls dann nicht der Fall, wenn der Vertrag eine Regelung enthält, die eine Datenherausgabe an weitere an der Gesellschaft Beteiligte ausdrücklich ausschließt.

Mindestens in dieser Fallgestaltung mit Ausschlussregelung erscheint es dem EuGH auch als zweifelhaft, dass eine Verarbeitungsbefugnis in Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO bestehen könnte. Es sei wahrscheinlich, dass die weiteren Beteiligten aufgrund einer solchen Ausschlussregelung zum Zeitpunkt der Erhebung Ihrer Daten nicht vernünftigerweise erwarten konnten, dass diese an weitere Beteiligte weitergegeben werden.

Im Ergebnis muss dies jedoch nun noch nicht bedeuten, dass hierdurch sämtliche Herausgaben durch entsprechende Vertragsklauseln ausgeschlossen werden können. Der EuGH überlässt es nämlich dem vorlegenden Gericht zu entscheiden, ob nicht die nationale Rechtsprechung (z. B. des BGH bezüglich der Unwirksamkeit entsprechender Vertragsklauseln) das deutsche Recht derart präzisiert, dass es selbst eine rechtliche Verpflichtung und damit eine datenschutzrechtliche Zulässigkeit nach Art. 6 Abs. 1 UAbs. 1 Buchstabe c) DS-GVO begründet.

Generell habe das vorlegende Gericht zudem auch noch näher zu prüfen, ob gegenüber der direkten Bekanntgabe der Daten an die anfragende Person, im Kontext der jeweiligen Zulässigkeitsnorm, nicht auch weniger eingreifende Mittel zur Erfüllung des Verarbeitungszwecks denkbar sind, wie z. B. eine Weiterleitung entsprechender Kontaktersuchen durch die Gesellschaft an die weiteren an der Gesellschaft Beteiligten, sodass diese jeweils selbst darüber entscheiden können, ob sie hierauf antworten und damit ihre Identität preisgeben.

Insofern zeigt der EuGH hier für bestimmte Fallkonstellationen zukünftig einen vertieften Prüfungsbedarf auf. Wie die nationalen Gerichte nun in den Fragen entscheiden, die der EuGH offen gelassen hat, bleibt abzuwarten.

6.3 Unzulässige Einholung von Einwilligungen zu Kontoverträgen

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

Bereits in unserem Tätigkeitsbericht 2022 hatten wir auf einen Fall aufmerksam gemacht, bei welchem eine Bank einen Betroffenen durch Vorankreuzungen und letztlich auch durch Zwang unzulässigerweise dazu bringen wollte, ihr eigentlich freiwillige datenschutzrechtliche Einwilligungen, z. B. zur individuellen werblichen Ansprache über verschiedene Kommunikationskanäle, zu erteilen. Für den Fall, dass er diese nicht erteile, wurde ihm eine Kündigung der Geschäftsbeziehung in Aussicht gestellt.

Da wir leider immer wieder mit Fallgestaltungen befasst sind, in welchen bei der Einholung datenschutzrechtlicher Einwilligungen die erforderliche Freiwilligkeit nicht berücksichtigt wird, möchten wir die hieraus entstehenden Folgen nochmals verdeutlichen.

Einwilligungserklärungen, bei welchen die Einwilligungsfelder durch den Verantwortlichen eigenmächtig vorbelegt / vorangekreuzt werden, oder bei denen der Abschluss oder Fortbestand der Vertragsbeziehung von der Erteilung abhängig gemacht wird, sind unwirksam.

Dies gilt ebenso, wenn Betroffene durch eine Vorspiegelung falscher Tatsachen und Erfordernisse zur Einwilligungserteilung gebracht werden. So hatten wir beispielsweise einen Vorgang zu bearbeiten, bei welchem den Betroffenen mitgeteilt wurde, dass die Erteilung der Einwilligungen benötigt werde, um die Sicherheit ihrer Daten zu gewährleisten. Tatsächlich handelte es sich jedoch um Einwilligungen zur Auswertung des Zahlungsverkehrs und weiteren Verarbeitungen zur individuellen werblichen Ansprache.

Bei der Sicherheit der Verarbeitung handelt es sich um eine Grundpflicht des Verantwortlichen (Art. 5 Abs. 1 Buchstabe f und Art. 32 DS-GVO), die dieser kraft Gesetzes, also völlig unabhängig von einer Einwilligung, zu gewährleisten hat.

Solche unwirksamen Einwilligungen sind nicht geeignet, eine Verarbeitung im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe a) DS-GVO zu legitimieren. Somit sind sämtliche Verarbeitungen, die auf solchen Einwilligungen basieren, datenschutzrechtlich unzulässig. Eine solche Unzulässigkeit kann dann auch nicht nachträglich für

die Vergangenheit geheilt werden, sollten Betroffene zu einem späteren Zeitpunkt noch eine rechtskonforme Einwilligung erteilen.

Insofern ist Verantwortlichen dringend anzuraten, ihre Prozesse zur Einwilligungserteilung kritisch zu prüfen.

Für weitere Details verweisen in diesem Zusammenhang auf Art. 7 DS-GVO i. V. m. der Leitlinie 05/2020 des Europäischen Datenschutzausschusses zur Einwilligung.

7

Werbung

7 Werbung

7.1 Anforderungen an einen klaren und deutlichen Hinweis auf die Widerspruchsmöglichkeit bei Bestandskundenwerbung

Im Rahmen der sog. Bestandskundenwerbung genügt es unseres Erachtens nicht, dass alleine in den Datenschutzhinweisen über die Bewerbung mit ähnlichen Waren oder Dienstleistungen und das Widerspruchsrecht informiert wird. Es bedarf eines klaren und deutlichen Hinweises unmittelbar bei Erhebung der Kontaktdaten.

Sollen Kontaktinformationen zum Zwecke der Versendung von Werbung mittels elektronischer Post (z. B. E-Mails, SMS, Messenger-Nachrichten) verarbeitet werden, bedarf es unter Einbeziehung der Wertung des § 7 Abs. 2 Nr. 2 UWG – Gesetz gegen den unlauteren Wettbewerb – grundsätzlich einer Einwilligung. Eine Ausnahme hiervon gilt jedoch bei der Datenverarbeitung zu Zwecken der sog. Bestandskundenwerbung. Bestandskundenbewerbung meint, eine Bewerbung von Kunden mit elektronischer Post unter Einhaltung der Anforderungen des § 7 Abs. 3 UWG. In diesen Fällen, ist die Verarbeitung und insbesondere Speicherung für diesen Zweck mit der Befugnis aus Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO begründbar; von einem überwiegenden Interesse der betroffenen Person wird dann in der Regel nicht ausgegangen.

§ 7 Abs. 3 UWG verlangt:

> *1. dass ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,*
>
> *2. -der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,*
>
> *3. der Kunde der Verwendung nicht widersprochen hat und der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.*

Gerade die Anforderung an einen klaren und deutlichen Hinweis auf die jederzeitige Widerspruchsmöglichkeit wird unserer Ansicht nach häufig nicht erfüllt. Zwar finden sich im Regelfall in den Datenschutzhinweisen sowie in den verschickten Mails Hinweise auf ein Widerspruchsrecht bzw. die Möglichkeit über einen Abmeldelink zu widersprechen. Allerdings liegt ein klarer, deutlicher und unmittelbarer Hinweis, wie ihn aus unserer Sicht das UWG verlangt, bei Erhebung der E-Mail-Adresse oftmals nicht vor.

Eine Information in den Datenschutzhinweisen alleine reicht nicht aus. Dies wird insbesondere bei Betrachtung des Wortlauts des Art. 13 der Richtlinie 2002/58/EG (eprivacy-Richtlinie), der mit § 7 UWG in das nationale deutsche Recht umgesetzt wurde, deutlich. Dieser regelt, dass *„eine natürliche oder juristische Person, wenn sie von ihren Kunden im Zusammenhang mit dem Verkauf eines Produkts oder einer Dienstleistung gemäß der Richtlinie 95/46/EG deren elektronische Kontaktinformationen für elektronische Post erhalten hat, diese zur Direktwerbung für eigene ähnliche Produkte oder Dienstleistungen verwenden [kann], sofern die Kunden klar und deutlich die Möglichkeit erhalten, eine solche Nutzung ihrer elektronischen Kontaktinformationen bei deren Erhebung und bei jeder Übertragung gebührenfrei und problemlos abzulehnen, wenn der Kunde diese Nutzung nicht von vornherein abgelehnt hat."* Erwägungsgrund 41 erläutert

hierzu, dass der Kunde bei Erlangung der Kontaktinformation über deren weitere Nutzung zum Zweck der Direktwerbung klar und eindeutig unterrichtet werden und die Möglichkeit erhalten sollte, diese Verwendung abzulehnen. Dem Kunden muss somit bei Erhebung der E-Mail-Adresse klar und deutlich die Möglichkeit eingeräumt werden, von vornherein widersprechen zu können.

So hat auch das Landgericht Paderborn am 12.03.2024, (Az.: 2 O 325/23) entschieden, dass es nicht genügt, wenn in der Datenschutzerklärung ausgeführt wird, dass die Kundendaten für Werbezwecke genutzt werden und sich der Empfänger von der E-Mail-Marketingkommunikation abmelden kann, insbesondere wenn dieser Hinweis ohne textliche Hervorhebung im Rahmen eines 26 Seiten umfassenden Schriftstücks enthalten ist. Das Gericht fordert zudem die Bereitstellung eines anklickbaren bzw. ankreuzbaren Kästchens („Ich widerspreche der Verwendung meiner persönlichen Daten zu Werbezwecken").

Sind nicht sämtliche Voraussetzungen des § 7 Abs. 3 UWG erfüllt, ist in der Konsequenz (weiterhin) eine Einwilligung für die Versendung von Werbung mittels E-Mail-Adresse nach § 7 Abs. 2 Nr. 2 UWG erforderlich. Einer solchen bedarf es dann ebenso für die Speicherung und Verarbeitung der E-Mail-Adresse, da in diesem Fall eine Befugnis gem. Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO aufgrund des Wertungsgleichklanges der Gesetze nicht angenommen werden kann.

8

Industrie und Handel

8 Industrie und Handel, Wohnungswirtschaft

8.1 Asset Deal/Share Deal - Update

Der überarbeitete DSK-Beschluss zum Asset Deal gibt Orientierung zum datenschutzgerechten Übergang insbesondere hinsichtlich der Kundendaten, aber auch hinsichtlich der Beschäftigtendaten.

Im Vergleich zu den vergangenen Jahren erhielten wir 2024 gehäuft Eingaben, die sich auf Datenverarbeitungen im Zusammenhang mit Asset- aber auch Share Deals bezogen.

Im Rahmen des Asset Deal waren die betroffenen Personen oftmals aufgrund der Informationen, die sie durch das veräußernde Unternehmen erhielten, verunsichert und richteten Nachfragen an uns. Oder die betroffenen Personen wurden direkt von dem erwerbenden Unternehmen kontaktiert, ohne dass sie zuvor Kenntnis von der Übernahme hatten.

Wie auch der überarbeitete Beschluss der Datenschutzkonferenz „Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals“ vom 11.09.2024 festhält, ist unter dem Begriff des Asset Deals *„(…)ein Unternehmenskauf zu verstehen, bei dem Wirtschaftsgüter/Vermögenswerte (engl.: Assets) eines Unternehmens wie beispielsweise Grundstücke, Gebäude, Maschinen, Kundenstamm, Rechte etc., im Rahmen der Singularsukzession auf die Erwerberin oder den Erwerber übertragen werden. Ein Asset Deal liegt zum Beispiel vor, wenn eine Einzelunternehmerin oder ein Einzelunternehmer (Veräußerer) ihren bzw. seinen Betrieb an eine Nachfolgerin oder einen Nachfolger (Erwerber) übergibt und dabei beispielsweise die Maschinen, den Kundenstamm, die Firmierung etc. übernimmt und den Betrieb fortführt.“*

An dieser Stelle sei darauf hingewiesen, dass der überarbeitete Beschluss der Datenschutzkonferenz nunmehr nicht nur eine Begriffsdefinition zum Asset Deal enthält, sondern vielmehr hinsichtlich der jeweils einschlägigen Rechtsgrundlagen differenziert und die Verarbeitung zu Werbezwecken, von Beschäftigten- und Lieferantendaten, von besonderen Kategorien personenbezogener Daten, von Bankdaten und von säumigen Kunden (Kundinnen und Kunden mit offenen Forderungen) behandelt.

Werden Kundendaten im Rahmen eines Asset Deals übermittelt, so ist zunächst zu unterscheiden, um welche Vertragsphase es geht (Vertragsanbahnung, laufende oder bereits beendete vertragliche Beziehungen). In den meisten von uns bearbeiteten Vorgängen wurden personenbezogene Kundendaten aus laufenden Vertragsbeziehungen im Rahmen einer Vertragsübernahme verarbeitet. Diese Phase wird angenommen, wenn der Veräußerer Verpflichtungen gegenüber einer Kundin oder einem Kunden aus einem Vertragsverhältnis hat bzw. gesetzliche Verjährungsfristen oder vertragliche Garantiepflichten noch nicht abgelaufen sind. Wurde die zivilrechtlich erforderliche Genehmigung für eine Vertragsübernahme erteilt, so ist eine Übermittlung der personenbezogenen Kundendaten durch den Veräußerer und die nachfolgende Verarbeitung durch den Erwerber auf Grundlage des Art. 6 Abs. 1 UAbs. 1 Buchstabe b) DS-GVO zulässig.

Diese Aufteilung in die Vertragsphasen sowie die rechtliche Bewertung weicht von dem bisherigen Beschluss der DSK insbesondere insofern ab als in dem Beschluss aus dem Jahr 2019 lediglich Fallgruppen aufgelistet wurden, die im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO zu beachten waren. Hierauf möchten wir aufmerksam machen und empfehlen die Lektüre des überarbeiteten Beschlusses.

Daneben stellte sich aber auch in einigen von uns bearbeiteten Beschwerdeverfahren insbesondere im Zusammenhang mit der Geltendmachung von Betroffenenrechten heraus, dass ein Share Deal vorlag, dem zudem eine Umfirmierung folgte. Ein Share Deal liegt dann vor, wenn Geschäftsanteile verkauft werden, das Unternehmen somit unverändert fortgeführt wird (Wechsel des/eines Eigentümers). Mangels Änderung des Verantwortlichen bestehen die datenschutzrechtlichen Pflichten fort und muss sich der Verantwortliche ein datenschutzwidriges Verhalten auch aus der Zeit vor dem Share Deal (weiterhin) zurechnen lassen.

Beschwerdeauslösend war in den von uns behandelten Fällen regelmäßig, dass die Bearbeitung von Betroffenenrechten nicht (mehr) erfolgte. Zumeist wurde dabei angeführt, dass die Anträge betroffener Personen nicht „weitergegeben" worden seien. Dies war jedoch keine Begründung dafür, vor dem Share Deal eingegangene Anträge nicht zu bearbeiten, sondern offenbarte vielmehr, dass Prozesse und interne Zuständigkeiten jedenfalls hinsichtlich der Umsetzung von Betroffenenrechten nicht etabliert waren und fortgeführt wurden.

8.2 Insolvenzverwalter als Auskunftverpflichteter

„Starke" vorläufige Insolvenzverwalter und Insolvenzverwalter sind Verantwortliche gem. Art. 4 Nr. 7 DS-GVO und sind deshalb grundsätzlich verpflichtet, einem Auskunftsbegehren nachzukommen.

Bei der Bearbeitung von Eingaben insbesondere bzgl. der Nicht-Erfüllung von Anträgen auf Auskunft gem. Art. 15 DS-GVO begegneten uns im Berichtszeitraum vermehrt Sachverhalte, in denen der Beschwerdegegner Insolvenz angemeldet hat und ein vorläufiger Insolvenzverwalter (§ 22 Insolvenzordnung - InsO) bestellt bzw. das Insolvenzverfahren bereits eröffnet wurde.

In diesen Verfahren richten wir uns regelmäßig an den (vorläufig bestellten „starken") Insolvenzverwalter (§ 56 InsO), die sich jedoch in den meisten Fällen nicht als Verantwortliche gem. Art. 4 Nr. 7 DS-GVO sehen.

Soweit es sich um einen vorläufigen Insolvenzverwalter nach § 22 InsO handelt, bewerten wir diesen dann als Verantwortlichen gem. Art. 4 Nr. 7 DS-GVO, wenn das Gericht neben der Verwalterbestellung ein allgemeines Verfügungsverbot erlassen hat („"starker" vorläufiger Insolvenzverwalter). Denn nur in diesem Fall geht die Verwaltungs- und Verfügungsbefugnis auf den Insolvenzverwalter über. Bei einem sog. „schwachen" vorläufigen Insolvenzverwalter bleibt hingegen (grundsätzlich) der Insolvenzschuldner Verantwortlicher.

Jedenfalls mit Eröffnung des Insolvenzverfahrens tritt der Insolvenzverwalter in die Stellung des Insolvenzschuldners ein, so dass ihn alle Pflichten treffen, außer es handelt sich um höchstpersönliche Pflichten des Insolvenzschuldners. Auch wenn das Recht auf Auskunft zwar ein höchstpersönliches Recht darstellt und daher nicht Teil der Insolvenzmasse werden kann, stellt es aber keine höchstpersönliche Pflicht dar, die nur der ursprüngliche Verantwortliche erfüllen könnte. Ab dem Zeitpunkt der Inbesitznahme (§ 148 InsO) der Daten bzw. Datenträger hat die Insolvenzverwalterin bzw. der Insolvenzverwalter die tatsächliche Entscheidungshoheit bezüglich der hiermit verbundenen Verarbeitungsprozesse innerhalb des insolventen Unternehmens inne und wird Verantwortlicher im datenschutzrechtlichen Sinne für die im Rahmen seiner Verwaltungstätigkeit vorgenommenen Verarbeitungstätigkeiten.

Damit trifft diesen auch die Pflicht diesbezügliche Auskunftsersuchen zu beantworten.

Gegen die Bewertung als Verantwortlicher wird häufig eine Entscheidung des AG Hamburg angeführt, (Urteil vom 15.11.2021 - 11 C 75/21), wonach der Insolvenzverwalter insbesondere

- lediglich eine überwachende Funktion habe,
- als Amtsperson im Sinne des deutschen Insolvenzrechtes bereits per se dem datenschutzrechtlichen Unionsrecht der DS-GVO nicht unterstellt sei,
- die Massegenerierungspflicht aus §§ 80, 148 InsO nicht etwa über Auskunftsersuchen gefährdet werden darf, indem er z. B. verpflichtet wäre, Verfahrensbeteiligten oder ehemaligen Verfahrensbeteiligten oder Organen der Insolvenzschuldnerin über deren -eingeschränkte- Akteneinsichtsrechte nach § 299 ZPO (§ 4 InsO) hinaus, weitere Auskünfte zu erteilen, die damit auf eine Auskunftserlangung in Daten über diejenigen aus der Insolvenzakte hinaus geeignet wären und u. U. zu einem prozessrechtlichen Vorteil der solcherart Auskunftsverlangenden in kontradiktorischen Massegenerierungsprozessen führen könnten und
- die Verarbeitung nicht „an Stelle" der Schuldnerin bzw. des Schuldners erfolge, da eine „Datenlagerung" keine Datenverarbeitung sei.

Dem ist jedoch entgegenzuhalten, dass insbesondere die Bereichsausnahme gem. Art. 2 Abs. 2 Buchstabe a DS-GVO in den vorliegenden Konstellationen nicht greift. Auch etwaige Konsequenzen führen nicht dazu, dass von der datenschutzrechtlichen Einordnung als Verantwortlicher für die im Rahmen der Insolvenzverwaltung vorgenommenen Verarbeitungstätigkeiten gem. Art. 4 Nr. 7 DS-GVO abzuweichen ist. Je nach Fallgestaltung kann die Auskunftsgewährung durch gesetzlich geregelte Ausnahmen (z. B. Art. 15 Abs. 4 DS-GVO bei Gefahr der erheblichen Verkürzung der Insolvenzmasse) eingeschränkt werden. Schließlich überzeugt auch der Verweis auf die bloße „Datenlagerung" nicht, soweit der Insolvenzverwalter bzw. die Insolvenzverwaltern jedenfalls die Möglichkeit hat, mit den personenbezogenen Daten umzugehen und damit über die für die Verantwortlichkeit gem. Art 4 Nr. 7 DS-GVO notwendige Einflussmöglichkeit auf die Datenverarbeitung verfügt.

Jeweils nach Erteilung der Auskunft haben wir im erforderlichen Umfang bei der abschließenden Bewertung des Vorganges die besondere Situation des Vorliegens eines Insolvenzverfahrens in die Entscheidung mit einbezogen und konnten wir so von unseren Befugnissen ermessensgerecht und verhältnismäßig Gebrauch machen. Weitere Besonderheiten bei der Bewertung eines vor Eintritt der Insolvenz geltend gemachten Auskunftsrechts, dessen Erfüllung gegen den Insolvenzverwalter durchgesetzt werden sollte, bleiben wegen eines noch anhängigen Rechtsstreits dem folgenden Berichtszeitraum vorbehalten.

8.3 Weiterleitung von E-Mails und Offenlegung personenbezogener Daten in Online-Portalen

Die Vorgaben des Datenschutzrechts gelten auch innerhalb von Wohnungseigentümergemeinschaften und Mietverhältnissen.

Im Berichtszeitraum erreichten uns mehrere Eingaben, in denen sich über die Weiterleitung von E-Mails von Mietern und Eigentümern durch Hausverwaltungen bzw. Vermieter, sowie die Offenlegung personenbezogener Daten von Wohnungseigentümern in Online-Portalen beschwert wurde.

Wie bereits gerichtlich mehrfach bestätigt sind die Vorschriften der DS-GVO auch bei Mietverhältnissen und innerhalb von Wohnungseigentümergemeinschaften anwendbar.

Weiterleitungen von E-Mails und die Offenlegung von personenbezogenen Daten in Form

von Verbrauchswerten oder Hausgeldzahlungen in Online-Portalen benötigen daher immer eine Rechtsgrundlage i. S. d. Art. 6 Abs. 1 DS-GVO. Durch die Verantwortlichen ist daher sorgfältig und für die jeweiligen Verarbeitungszwecke einzeln zu prüfen, ob eine solche Rechtsgrundlage besteht. Diese ist zu dokumentieren und im Rahmen der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachzuweisen.

In Bezug auf Wohnungseigentümergemeinschaften gelten bestimmte Besonderheiten, die sich auch in datenschutzrechtlicher Hinsicht auswirken. So sehen wir es grundsätzlich als zulässig an, wenn Eigentümerlisten bzw. Namen und Adressen der Eigentümer durch die Hausverwaltung innerhalb der Wohnungseigentümergemeinschaft offenbart werden. Denn in der Rechtsprechung ist anerkannt, dass die Wohnungseigentümergemeinschaft keine anonyme Gemeinschaft ist und der einzelne Eigentümer berechtigt ist, die Identität und Anschrift der anderen Wohnungseigentümer zu erfahren.

Betreffend die einzelnen E-Mail-Adressen sehen wir allerdings keine entsprechende Notwendigkeit. Die Offenlegung von E-Mail-Adressen, insbesondere durch Weiterleitungen mit offenem Verteiler, ist daher grundsätzlich nur mit einer Einwilligung der betreffenden Personen zulässig. Ob eine solche Einwilligung dadurch erteilt wird, dass E-Mail-Adressen in der Eigentümergemeinschaft zirkuliert werden, hängt vom jeweiligen Einzelfall und den Gepflogenheiten innerhalb der Eigentümergemeinschaft ab.

Ferner kann bei der Offenlegung von Nachrichten von Wohnungseigentümern bzw. deren Mieter an die Hausverwaltung gegenüber allen Wohnungseigentümern ein Verstoß gegen den Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO vorliegen. Häufig ist es nicht erforderlich das Schreiben an sich weiterzuleiten, sondern es genügt mitunter die inhaltlich angesprochenen Themen zu kommunizieren.

Auch hinsichtlich der Offenlegung von personenbezogenen Daten wie Verbrauchswerten oder Hausgeldzahlungen innerhalb der Wohnungseigentümergemeinschaft gelten Besonderheiten. Denn nach den Vorgaben des Wohnungseigentumsgesetzes besitzt jeder Eigentümer gegenüber der Wohnungseigentümergemeinschaft einen Anspruch auf Einsicht in die Verwaltungsunterlagen (sog. Belegeinsicht – § 18 Abs. 4 WEG). Dieser Anspruch wird regelmäßig im Innerverhältnis durch die beauftragte Hausverwaltung erfüllt. Auch ist die Kenntnis der entsprechenden Einzelabrechnungen erforderlich, damit die Gemeinschaft der Wohnungseigentümer etwaige Nachschüsse bzw. Anpassungsbeiträge zur Jahresgesamtabrechnung beschließen kann. Insoweit sehen wir datenschutzrechtlich keinen Verstoß, wenn die Hausverwaltung in diesem Rahmen den einzelnen Eigentümern die Abrechnungsunterlagen und Einzelabrechnungen zur Verfügung stellt. Voraussetzung dafür ist aber natürlich, dass auch Einsicht in die Verwaltungsunterlagen verlangt wurde und die Zurverfügungstellung nicht automatisch erfolgt.

Im Zusammenhang mit konkreten Beschwerdeverfahren ist uns zudem aufgefallen, dass Hausverwaltungen zur Einsicht in Verwaltungsunterlagen häufig Online- Portale einsetzen. Hierzu werden regelmäßig nicht selbst entwickelte Softwarelösungen eingesetzt, die zu diesem Zweck eingekauft werden. Hierbei ist zu beachten, dass die datenschutzrechtliche Verantwortlichkeit grundsätzlich bei den einsetzenden Hausverwaltungen liegt, da diese die Software für ihre Zwecke einsetzen und über die diesbezüglichen Mittel der Verarbeitung entscheiden. Die Softwarehersteller sind insoweit als Auftragsverarbeiter gem. Art. 4 Nr. 8 DS-GVO einzuordnen. Hierauf wurde unsererseits in den jeweiligen Beschwerdeverfahren nochmals besonders aufmerksam gemacht.

9

Beschäftigtendatenschutz

9 Beschäftigtendatenschutz

9.1 Datenverarbeitung des Arbeitgebers im Rahmen des Annahmeverzugslohns

Ein Auskunftsanspruch des Arbeitgebers gegenüber dem Arbeitnehmer, zur Begründung von Einwendungen nach § 11 Satz 2 Kündigungsschutzgesetz (KSchG) setzt voraus, dass die Geltendmachung von Annahmeverzugslohn konkret absehbar ist.

Im Berichtszeitraum erreichten uns mehrere Beschwerden und Anfragen von Beschäftigten, in denen es insbesondere darum ging, ab welchem Zeitpunkt eine Auskunft zu z. B. seitens der Agentur für Arbeit bzw. des Jobcenters erhaltenen Stellenangeboten und den Bewerbungsbemühungen eines gekündigten Arbeitnehmers durch den Arbeitgeber verlangt werden darf. In allen Fällen befanden sich die Eingabeführer entweder kurz vor oder in einem Kündigungsschutzprozess, d. h. die Entscheidung, inwieweit die Kündigung wirksam gewesen ist, war noch nicht gefallen.

Soweit das Gericht nämlich feststellen sollte, dass die Kündigung unwirksam gewesen ist, schuldet der Arbeitgeber dem Arbeitnehmer ab dem Zeitpunkt der Entlassung (Zeitpunkt zu dem die Kündigung greifen sollte) dessen Arbeitslohn. Allerdings muss sich der Beschäftigte gem. § 11 Satz 2 KSchG unter anderem das anrechnen lassen, was er in der Zeit nach der Entlassung hätte verdienen können, soweit er die Annahme einer zumutbaren Arbeit nicht böswillig unterlassen hatte, er also in Kenntnis aller objektiven Umstände vorsätzlich untätig blieb bzw. verhinderte, eine Stelle angeboten zu bekommen. Der Arbeitnehmer muss also entweder eine ihm bekannte zumutbare Tätigkeiten annehmen oder aber sich den potentiellen Verdienst aus einer ihm zumutbaren Tätigkeit anrechnen lassen.

Da es jedoch einem Arbeitgeber im Regelfall nicht möglich ist, vorzutragen, welche zumutbaren Stellen dem Arbeitnehmer angeboten wurden und inwieweit er böswillig deren Annahme unterlassen hat bzw. durch entsprechendes Verhalten verhindert hat, solche Stellen angeboten zu bekommen, können nach der arbeitsrechtlichen Rechtsprechung Informationen vom Arbeitnehmer gefordert werden. Eine Erhebung und weitere Verarbeitung der damit zusammenhängenden personenbezogenen Daten ist in diesem Zusammenhang dann grundsätzlich zulässig (Art. 6 Abs. 1 UAbs. 1 Buchstabe b) DS-GVO, ggf. in Verbindung mit Art. 9 DS-GVO, § 26 Abs. 3 BDSG).

In den uns vorliegenden Fällen war jedoch zum Zeitpunkt der arbeitgeberseitigen Aufforderung zur Beauskunftung noch nicht entschieden, ob das Arbeitsverhältnis durch die Kündigung zum entsprechenden Kündigungszeitpunkt beendet wird/wurde bzw. war unklar, ob eine Beendigung des Rechtsstreits durch einen Vergleich erfolgt und inwieweit überhaupt noch ein Anspruch auf Annahmeverzugslohn geltend gemacht wird.

Auch wenn in dem Einlegen einer Kündigungsschutzklage i. d. R. eine konkludente Geltendmachung von Annahmeverzugslohn gesehen wird (um Ausschlussfristen zu wahren), konnten wir zu diesem Zeitpunkt noch keine Befugnis des Verantwortlichen hinsichtlich der Verarbeitung der angeforderten personenbezogenen Daten erkennen. Dies begründet sich damit, dass zu diesem Zeitpunkt noch nicht absehbar war, ob ein Annahmeverzugslohn überhaupt geltend gemacht werden kann oder wird. Folglich konnte auch nicht festgestellt werden, dass die Erforderlichkeit für die Verarbeitung der

personenbezogenen Daten aus den Bewerbungsunterlagen, aber auch aus den nähren Umständen der Bewerbungsverfahren, vorlag.

9.2 Datenverarbeitung durch den Betriebsrat

Gemäß § 79a Betriebsverfassungsgesetz (BetrVG) trifft den Betriebsrat bei der Erfüllung seiner Aufgaben eine Pflicht zur Unterstützung des Arbeitgebers bei der Einhaltung der datenschutzrechtlichen Vorschriften.

Innerhalb des Berichtszeitraumes hatten wir einige Eingänge zu verzeichnen, in denen Arbeitgeber aufgrund fehlender Unterstützung des Betriebsrates nur schwerlich ihren datenschutzrechtlichen Pflichten nachkommen konnten.

Gemäß § 79a S. 2 BetrVG ist der Arbeitgeber auch dann Verantwortlicher, wenn und soweit der Betriebsrat zur Erfüllung der in seiner Zuständigkeit liegenden Aufgaben personenbezogene Daten verarbeitet. Allerdings müssen sich der Arbeitgeber und der Betriebsrat gegenseitig bei der Einhaltung der datenschutzrechtlichen Vorschriften unterstützen (vgl. § 79a S. 3 BetrVG).

Wird zum Beispiel ein Auskunftsersuchen gem. Art. 15 DS-GVO gegenüber dem Arbeitgeber geltend gemacht, so muss dieser grundsätzlich, soweit keine Ausnahme von der Auskunftsverpflichtung besteht, auch die Datenverarbeitungen zu der betroffenen Person, die durch den Betriebsrat erfolgten, beauskunften. In dieser Konstellation weigern sich jedoch manche Betriebsräte dem Arbeitgeber eine entsprechende (Teil-)Auskunft zur Verfügung zu stellen und begründen dies mit ihrer besonderen Stellung und ihrer Verschwiegenheitsverpflichtung. Eine praktikable Möglichkeit, einem Auskunftsersuchen vollumfänglich nachzukommen ist es aus hiesiger Sicht, wenn entweder der Betriebsrat selbst der betroffenen Person die entsprechende (Teil-) Auskunft zur Verfügung stellt oder wenn die oder der Datenschutzbeauftragte eingebunden wird. So bestimmt § 79a BetrVG in Satz 4, dass die oder der Datenschutzbeauftragte gegenüber dem Arbeitgeber zur Verschwiegenheit verpflichtet ist über Informationen, die Rückschlüsse auf den Meinungsbildungsprozess des Betriebsrats zulassen. Die oder der Datenschutzbeauftragte ist somit nicht für ein „Lager" beratend und unterstützend tätig, sondern kann ggf. auch als quasi neutrale vertrauensvolle Stelle innerhalb des Verantwortlichen agieren, ggf. die (Teil-)Auskünfte zusammenführen und diese an die betroffene Person versenden. Mit diesen Empfehlungen konnten wir einige Verfahren praktikabel und zielorientiert begleiten.

Ähnliche Argumentationen der Betriebsräte werden zum Teil auch vorgetragen, wenn wir eine Stellungnahme gem. Art. 58 Abs. 1 Buchstabe a) DS-GVO von einem Verantwortlichen anfordern und dieser innerhalb seines Unternehmens der Beschwerde nachgeht. Teilweise wird uns dann mitgeteilt, dass eine vollumfängliche Stellungnahme nicht abgegeben werden kann, da sich der Betriebsrat weigern würde, mitzuwirken. Aber auch hier trifft den Betriebsrat eine Pflicht zur Unterstützung des Arbeitgebers bei der Einhaltung datenschutzrechtlicher Vorschriften.

Bei der Frage der Durchsetzung der Unterstützungspflicht handelt es sich jedoch unseres Erachtens um eine arbeitsrechtliche Fragestellung, so dass es einer zivilrechtlichen Klärung bedarf. Aus diesem Grund lassen wir uns dann, wenn eine arbeitgeberseitige Stellungnahme dahin geht, dass eine vollständige Aufarbeitung einer Datenverarbeitung und Abgabe einer entsprechenden Stellungnahme mangels Mitwirkung des Betriebsrats nicht möglich ist, zunächst darlegen, welche Schritte seitens des Arbeitgebers unternommen wurden um den datenschutzrechtlichen Pflichten, insbesondere der Einhaltung der datenschutzrechtlichen Vorgaben,

nachzukommen. Soweit im konkreten Einzelfall angemessene Schritte unternommen wurden, fließt dies in dann in unserer (abschließenden) Bewertung mit ein.

9.3 Umgang mit der Veröffentlichung von Bildnissen Beschäftigter nach Beendigung des Beschäftigungsverhältnisses

Sollen Bildmaterialien, auf denen Beschäftigte abgebildet sind, nach Beendigung des Beschäftigtenverhältnisses weiterhin veröffentlicht werden, sollte dies bereits im Vorfeld vertraglich vereinbart werden.

Wird ein Arbeitsverhältnis beendet, muss der Arbeitgeber prüfen, welche personenbezogenen Daten des Beschäftigten er noch weiterhin wie verarbeiten darf. In zahlreichen im Berichtszeitraum bearbeiteten Verfahren konnten wir feststellen, dass die Beschäftigtendaten auch nach Beendigung des Beschäftigtenverhältnisses weiterhin verarbeitet werden, ohne dass eine Befugnis hierfür vorlag.

Sehr häufig erreichten uns beispielsweise Beschwerden dazu, dass auch nachdem ein Beschäftigter aus einem Unternehmen ausgeschieden ist, Fotos und Videos die (auch) den Beschäftigten zeigen weiterhin auf der Homepage und insbesondere auf verschiedenen Social-Media-Plattformen veröffentlicht wurden.

In der Regel erfolgt die Veröffentlichung von Fotos oder Filmaufnahmen von Beschäftigten auf Grundlage einer Einwilligung des Beschäftigten. Wird das Arbeitsverhältnis beendet, kann eine weitere Veröffentlichung der Beschäftigtendaten grundsätzlich nicht mehr auf die Einwilligung gestützt werden, da diese üblicherweise für einen bestimmten Zweck (z. B. positive und nahbare Darstellung des Unternehmens) erteilt und jedenfalls nach Auslegung der ursprünglich erteilten Willenserklärung des Beschäftigten gem. §§ 133, 157 BGB für den Zeitraum, in dem der Beschäftigte für den Arbeitgeber tätig war, abgegeben wurde. In den von uns bearbeiteten Fällen wurden erteilte Einwilligungen zudem ausdrücklich gem. Art. 7 Abs. 3 DS-GVO widerrufen. Bildmaterialien sind in beiden Fällen (Wegfall der Zweckbindung gem. Art. 5 Abs. 1 Buchstabe b) DS-GVO sowie Widerruf der Einwilligung gem. Art. 7 Abs. 3 DS-GVO) unverzüglich zu löschen, soweit eine anderweitige Rechtsgrundlage für die Verarbeitung nicht vorliegt (vgl. Art. 17 Abs. 1 Buchstabe a) bzw. b) DS-GVO).

In einem von uns bearbeiteten Vorgang beschwerte sich die Beschwerdeführerin darüber, dass ihr ehemaliger Arbeitgeber weiterhin Bilder und Videos von ihr in den sozialen Medien veröffentlicht, obwohl sie ihren Arbeitgeber bereits zur Löschung aufgefordert hatte. Der Arbeitgeber weigerte sich, die Bilder und Videos zu löschen. Er führte an, dass ihm laut Arbeitsvertrag die Arbeitsergebnisse aus der Tätigkeit der Beschäftigten zustünden. Die Beschäftigte habe sich selbst zur Verfügung gestellt und sei mit den Bildaufnahmen und Veröffentlichungen einverstanden gewesen. Zudem sei ein hoher Betrag in den Ausbau der Marke, unter anderem auch in die Produktion der Bilder und Videoclips, in dem (auch) die Beschwerdeführerin zu sehen ist, investiert worden.

Da wir in dem konkreten Fall weder erkennen konnten, dass die (weitere) Veröffentlichung nach Beendigung des Beschäftigtenverhältnisses mit der arbeitsvertraglichen Regelung begründbar war und auf Grundlage des Art. 6 Abs. 1 UAbs.1 Buchstabe b) DS-GVO zulässig gewesen wäre noch, dass eine solche aufgrund des überwiegenden Interesses der Beschwerdeführerin gem. Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO rechtmäßig erfolgen konnte und auch eine etwaig gegebene Einwilligung aufgrund des Widerrufs nicht mehr weiterhin Grundlage für die Datenverarbeitung sein konnte, wiesen wir den Arbeitgeber unter Androhung eines

Zwangsgeldes an, die Fotos und Videosequenzen, auf denen die Beschwerdeführerin zu sehen ist, zu löschen. Gegen diesen Bescheid legte der ehemalige Arbeitgeber Klage ein und beantragte die Aufhebung desselben. Die Entscheidung des Bayerischen Verwaltungsgerichts Ansbach steht derzeit noch aus.

Soweit Bilder und Videomaterial Beschäftigtendaten enthalten und diese gegebenenfalls auch über das Bestehen eines Beschäftigtenverhältnisses hinaus verarbeitet werden sollen, empfehlen wir den Abschluss eines Model-Release-Vertrages. Mit einem solchen Vertrag können das Model/die abgebildete Person und der Vertragspartner (hier Arbeitgeber) regeln, wie die Personenabbildungen verwendet werden dürfen und welche Vergütung das Model hierfür erhält. In diesem Fall kann die (vertragsgemäße) Verarbeitung der Bildmaterialien auf Art. 6 Abs.1 UAbs. 1 Buchstabe b) DS-GVO gestützt werden.

10

Videoüberwachung

10 Videoüberwachung

10.1 Videoüberwachung in Nahversorgungs- und Automatenläden

Eine Videoüberwachung in Ladenlokalen muss auch dann, wenn diese (nahezu) personallos geführt werden, den Anforderungen des Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO genügen.

Ländliche Nahversorgungsläden, bei denen die entnommenen Produkte mittels Geldeinlage in eine Kasse bzw. Box erfolgt, sowie Automatenshops, die rund um die Uhr geöffnet sind (24/7) kommen größtenteils ohne Personal aus. Um aber insbesondere Beweismaterial für den Fall von Vandalismus oder Diebstählen zur Verfügung zu haben, betreiben einige Verantwortliche eine Videoüberwachungsanlage. Im Berichtszeitraum erreichten uns mehrere Anfragen zu den datenschutzrechtlichen Rahmenbedingungen einer entsprechenden Videoüberwachung.

Als Rechtsgrundlage für die Überwachung von Kunden, Begleitpersonen und Lieferanten, sowie ggf. miterfasstem Personal (z. B. beim Einräumen der Regale/Automaten) kommt Art. 6 Abs. 1 UAbs. 1 Buchstabe f) DS-GVO in Betracht, wonach eine Datenverarbeitung dann zulässig ist, wenn diese zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person nicht überwiegen.

Der Verantwortliche muss somit zunächst ein konkretes eigenes berechtigtes Interesse haben oder ein entsprechendes Dritt-Interesse an der Videoüberwachung vorweisen können. Ein solches kann angenommen werden, wenn eine konkrete Gefahrenlage vorliegt, die über ein allgemeines Lebensrisiko bzw. Geschäftsrisiko hinausgeht. Wird beispielsweise das Ziel verfolgt, Vandalismusvorfälle oder Diebstähle „auf Band" zu haben, um dies dann, wenn ein entsprechender Fall eintritt, den Ermittlungsbehörden zu übergeben, so müsste die erhöhte Gefahrenlage konkret begründbar und uns gegenüber nachweisbar sein. Dies könnte z. B. mit Vorfällen in der Vergangenheit bzw. Vorfällen in anderen, ähnlichen Konstellationen, in besonders gefahrengeneigten Bereichen (z. B. Partymeile, wenn ein erhöhtes Risiko von Vandalismus besteht) erfolgen. Auf Grundlage der Tatsachenbasis ist eine Prognoseentscheidung zu fällen, inwieweit (künftig) eine erhöhte Gefahrenlage gegeben ist.

Kann ein berechtigtes Interesse hiernach bejaht werden, muss die Datenverarbeitung mittels Videoüberwachungsanlage zudem erforderlich sein. Dies bedeutet, dass die Videoüberwachung geeignet sein muss, um dem Interesse zu dienen und es keine gleich geeigneten, aber mildere Maßnahmen geben darf. Hierbei ist nicht nur die Frage danach zu stellen, ob eine Videoüberwachung insgesamt erforderlich ist, sondern auch, in welchem Umfang eine solche erforderlich ist. Dies betrifft insbesondere die Frage nach den Erfassungsbereichen, die Überwachungszeiten und die Speicherdauer. Erfasst werden dürfen nur die Bereiche, in denen die entsprechenden Vorfälle, die aufgezeichnet werden sollen, geschehen können. Zeitlich ist die Videoüberwachung auf die Zeiträume einzugrenzen, in denen tatsächlich eine erhöhte Gefahrenlage besteht, d. h. beispielsweise. an Wochenenden, während der Nachtstunden o. ä. Grundsätzlich wird dann, wenn eine Dokumentation zu Beweiszwecken bezweckt werden soll, alleine eine Aufzeichnung und nicht zugleich eine Live-Überwachung ausreichend sein. Die Videoaufzeichnungen sind dann, wenn keine Vorfälle stattfanden, zeitnah zu löschen. Üblicherweise wird eine Speicherdauer von 72 h als

ausreichend erachtet. Soweit Auszüge an die Ermittlungsbehörden weitergegeben werden sollen, können diese ggf. länger aufbewahrt werden, soweit dies erforderlich ist.

Zuletzt dürfen die Rechte und Grundfreiheiten der betroffenen Person nicht überwiegen. In diese Interessenabwägung sind insbesondere der Anlass und die Umstände der Verarbeitung und die Folgen der Verarbeitung, sowie die Erwartungshaltung betroffener Personen einzustellen und den berechtigten Interessen des Verantwortlichen (oder eines Dritten) gegenüber zu stellen.

Im Ergebnis haben wir die Videoüberwachung der Ladenlokale in den von uns behandelten Vorgängen als zulässig bewertet.

Dabei treffen den Verantwortlichen Informationspflichten gem. Art. 13 DS-GVO. Der Verantwortliche muss also die betroffenen Personen jedenfalls mit einem sogenannten vorgelagerten Hinweisschild auf die Videoüberwachung hinweisen und die wichtigsten Informationen bereitstellen. Daneben muss zugleich darauf hingewiesen werden, wo diese abgerufen werden können (z. B. Homepage).

Nähere Informationen zur Videoüberwachung sowie Muster für Hinweisschilder finden sich in der Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen der Datenschutzkonferenz vom Juli 2020.

11

Gesundheit und Soziales

11 Gesundheit und Soziales

11.1 Recht auf kostenfreie Kopie der Patientenakte

Verantwortliche, die zum Führen einer Patientenakte verpflichtet sind, haben betroffenen Personen eine kostenfreie Erstkopie der Patientenakte zu erteilen.

Mit Urteil vom 26.10.2023 (Az. C-307/22) hat der Europäische Gerichtshof (EuGH) klargestellt, dass das Recht auf eine kostenlose Erstkopie der Patientenakte aus Art. 15 Abs. 3 Satz 1 DS-GVO nicht durch eine nationale Regelung, wie bspw. § 630g Abs. 2 Satz 2 Bürgerliches Gesetzbuch (BGB), eingeschränkt werden kann. Das Gericht bestätigt damit den Anspruch von Patientinnen und Patienten auf eine unentgeltliche erste Kopie ihrer Patientenakte. Entsprechende Anpassungen der bestehenden nationalen Rege-lungen stehen noch aus.

Im Berichtszeitraum haben wir vermehrt Beschwerden erhalten, wonach Ärztinnen und Ärzte weiterhin Kosten für die erste Kopie der Patientenakte verlangen. In einem besonders gravierenden Fall wurde uns berichtet, dass die Herausgabe der Akte von einer vorherigen Barzahlung in der Praxis abhängig gemacht wurde. Dies führte zu einer Verzögerung von über sechs Monaten, bis die Akte schließlich durch unser Eingreifen ausgehändigt wurde.

Ein solches Vorgehen entspricht, wie oben bereits erläutert, nicht den Vorgaben der DS-GVO. In allen betroffenen Fällen haben wir die Verantwortlichen auf die geltende Rechtslage hingewiesen. Nach kostenfreier Erteilung der Kopie wurden die Verfahren jeweils mit einer kostenpflichtigen Verwarnung gemäß Art. 58 Abs. 2 Buchstabe b) DS-GVO abgeschlossen.

11.2 Auskunftsanspruch eines Elternteils gegenüber dem gerichtlich bestellten Verfahrensbeistand seiner Kinder

Eltern können keinen Auskunftsanspruch im Namen ihres Kindes nach Art. 15 DS-GVO gegenüber dem Verfahrensbeistand durchsetzen; im Rahmen des eigenen Auskunftsanspruch des Elternteils sind nur die Stammdaten zu beauskunften.

Ein Elternteil beantragte gegenüber dem gerichtlich bestellten Verfahrensbeistand seiner Kinder Auskunft nach Art. 15 DS-GVO bezüglich der personenbezogenen Daten der Kinder sowie hinsichtlich seiner eigenen personenbezogenen Daten. Dem Auskunftsersuchen kam der Verfahrensbeistand nicht nach und verweigerte diese aufgrund der entgegenstehenden Interessen der Kinder, welcher dieser im Rahmen seiner Stellung als Verfahrensbeistand zu vertreten und zu wahren hat. Daraufhin legte das Elternteil Beschwerde bei uns ein.

Nach § 158 Abs. 1 Satz 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) hat das Gericht von Amts wegen dem minderjährigen Kind in Kindschaftssachen, die seine Person betreffen, einen fachlich und persönlich geeigneten Verfahrensbeistand zu bestellen, soweit dies zur Wahrnehmung der Interessen des Kindes erforderlich ist. Nach § 158b Abs. 1 Satz 1 FamFG gehört es zu den originären Aufgabenreich eines Verfahrensbeistands das Interesse des Kindes festzustellen (Erforschung der Wünsche, Bedürfnisse und Vorstellungen des Kindes) und im gerichtlichen Verfahren zur Geltung zu bringen. Der Verfahrensbeistand ist demnach sowohl dem Willen (subjektive Interesse) als auch dem Wohl (objektives Interesse) des Kindes verpflichtet und damit auch dem

verfassungsmäßig geschützten Recht des Kindes auf informationelle Selbstbestimmung.

Es würde gerade keiner sachgerechten Wahrnehmung der Interessen des Kindes sowie dessen Recht auf informationelle Selbstbestimmung entsprechen, wenn ein Verfahrensbeistand personenbezogen Daten des Kindes gegenüber einem Elternteil zu beauskunften hätte. Wie bereits aus dem gesetzlich definierten Aufgabenkreis des Verfahrensbeistands nach § 158b FamFG folgt, ist bei der beruflichen Tätigkeit eines Verfahrensbeistands der Schutz der Vertrauenssphäre notwendig, da dieser die Interessen des Kindes festzustellen und diese im gerichtlichen Verfahren zur Geltung zu bringen hat. Eine Auskunftserteilung hinsichtlich der personenbezogenen Daten des Kindes gegenüber einem Elternteil würde dem mit der Tätigkeit eines Verfahrensbeistands immanenten Vertrauensschutz entgegenstehen, so dass nach unser Auffassung ein Verfahrensbeistand die Auskunftserteilung bezüglich der personenbezogenen Daten des Kindes gegenüber dem antragstellendem Elternteil nach Maßgabe des § 29 Abs. 1 Satz 2 Alt. 2 BDSG verweigern kann.

Diese Erwägungen sind natürlich auch hinsichtlich des Auskunftsverlangens eines Elternteils gegenüber dem Verfahrensbeistand betreffend seine eigenen personenbezogenen Daten zu berücksichtigen. Es würde dem berechtigten und schützenswerten Interesse des Kindes an Geheimhaltung seiner personenbezogenen Daten zuwiderlaufen, wenn ein Elternteil im Rahmen seines im eigenen Namen gestellten Auskunftsantrag nach Art. 15 DS-GVO Kenntnis über sensible Inhalte erlangt, welche das Interesse des Kindes betreffen und somit die Vertrauenssphäre zwischen dem Kind und seinem Verfahrensbeistand konterkarieren würde. Nach unserer Auffassung beschränkt sich daher das Auskunftsrecht eines Elternteils gegenüber dem Verfahrensbeistand seiner Kinder bezüglich seiner eigenen personenbezogenen Daten daher nur auf die sog. „Stammdaten". Der Beauskunftung der „weiteren" personenbezogenen Daten des Elternteils steht die gesetzliche Wertung des § 29 Abs. 1 Satz 2 Alt. 2 BDSG entgegen.

11.3 Löschungsrechte nach Identitätsdiebstahl

Kein Löschungsrecht der betroffenen Person nach Art. 17 DS-GVO bei Identitätsdiebstahl.

Im Berichtszeitraum haben uns vermehrt Beschwerden erreicht, bei denen die beschwerdeführenden Personen angaben, Opfer eines Identitätsdiebstahl geworden zu sein, da eine unbekannte Person unter Verwendung ihrer Daten einen Versicherungsvertrag abgeschlossen hatte. Dies war aufgefallen, als sie Zahlungsaufforderungen von Versicherungsunternehmen erhielten, obwohl sie selbst keine Vertragsbeziehung eingegangen waren. Die beschwerdeführenden Personen beantragten daraufhin die Löschung ihrer personenbezogenen Daten vom Verantwortlichen.

Allerdings greift hier der Löschanspruch aus Art. 17 DS-GVO zunächst nicht, da zum Zeitpunkt der Antragsstellung zumeist noch unklar ist, ob und zwischen wem eine Vertragsbeziehung zustande gekommen ist. Solange der Verantwortliche glaubt gegenüber der betroffenen Person eine Forderung zu besitzen bzw. zumindest solange diese Möglichkeit besteht, kann die Datenspeicherung und Verwendung auf Art. 6 Abs. 1 UAbs. 1 Buchstabe b) DS-GVO gestützt werden, da diese Vorschrift die Verarbeitung personenbezogener Daten für zulässig erklärt, wenn die Verarbeitung zur Durchführung eines Vertrages erforderlich ist.

Erst wenn zivilrechtlich geklärt ist (bzw. sofern der Verantwortliche von der Verfolgung absieht, ggf. schon früher), dass kein Anspruch gegen die beschwerdeführende Person besteht, hat der Verantwortliche die Daten zu löschen.

11.4 Berichtigung von Sachverständigengutachten

Ob ein Sachverständigengutachten korrekt ist, können wir nur bei objektiv überprüfbaren Daten beurteilen. Die Prüfung der fachlichen Beurteilung des Sachverständigen fällt hingegen nicht in den Zuständigkeitsbereich der Datenschutzaufsicht.

Mitunter wenden sich Betroffene an uns, weil sie die in einem sie betreffenden Gutachten getroffenen Feststellungen für fehlerhaft halten und daher eine Berichtigung gemäß Art. 16 DS-GVO verlangen. Häufig handelt es sich dabei um medizinische oder psychiatrische Gutachten im Zusammenhang mit sozialgerichtlichen oder verwaltungsrechtlichen Verfahren sowie um Gutachten, die von Versicherungen zur Beurteilung von Leistungsfällen in Auftrag gegeben wurden – etwa Unfall- oder Schadensgutachten.

Nach Art. 16 DS-GVO haben Betroffene das Recht, unrichtige personenbezogene Daten berichtigen zu lassen. Unsere datenschutzrechtliche Zuständigkeit beschränkt sich jedoch auf die Prüfung objektiv feststellbarer Tatsachen, wie beispielsweise Kontaktdaten oder die Krankenversicherungsnummer der Eingabeführenden. Die fachliche Beurteilung eines Sachverhalts kann hingegen nicht durch uns überprüft werden, da diese nicht objektiv überprüfbar ist. Es handelt sich hierbei um eine subjektive Einschätzung, die dem Berichtigungsanspruch nicht unterliegt.

Die Klärung der Richtigkeit solcher Einschätzungen kann daher in der Regel nur durch eine erneute Begutachtung, beispielsweise im Rahmen eines Gerichtsverfahrens, erfolgen.

12

Datenschutz im Internet

12 Datenschutz im Internet

12.1 Veröffentlichungen im Internet

Die Veröffentlichung von personenbezogenen Daten Dritter im Internet kann im Regelfall nicht auf die Rechtsgrundlage des berechtigten Interesses gestützt werden und erfolgt daher zumeist rechtswidrig.

Neben Veröffentlichungen von rechtswidrigen Inhalten auf Online- Plattformen, beschäftigten uns im vergangenen Berichtszeitraum mehrfach rechtswidrige Veröffentlichungen in eigens dafür geschaffenen Internetauftritten, im Rahmen von Blogs usw.

Das Motiv für die Veröffentlichung war dabei meist in einer persönlichen Auseinandersetzung des Verantwortlichen mit der betroffenen Person oder einem erfahrenen vermeintlichen Unrecht zu sehen, über das die Öffentlichkeit informiert werden sollte oder über eine Öffentlichkeitswirksamkeit ein gewisser Druck auf den vermeintlichen „Schuldigen" ausgeübt werden sollte. Das Spektrum war dabei weit gespannt und reicht von Eltern, die über eine angeblich ungerechte Behandlung ihrer Kinder durch konkret benannte Lehrkräfte in der Schule berichten, über Personen, die negative Erfahrungen mit namentlich benannten Sachbearbeitern in Behörden/Unternehmen schildern oder Privatpersonen, die sich gegenseitiges Schikanieren bis hin zum Stalking vorwerfen.

In diesen Fällen ist der Anwendungsbereich der DS-GVO eröffnet, auch wenn es sich letztlich um private Auseinandersetzungen handelt, da eine Veröffentlichung im Internet für einen nicht begrenzbaren Adressatenkreis nicht der sog. Haushaltsausnahme des Art. 2 Abs. 2 Buchstabe c) DS-GVO unterfällt (siehe hierzu auch den Beitrag 4.1 in unserem 12. Tätigkeitsbericht aus dem Jahr 2022).

Die Veröffentlichung von personenbezogenen Daten, unabhängig davon, ob es sich hierbei um Fotos oder Texte handelt, stellt eine Verarbeitung personenbezogener Daten dar, die einer Rechtsgrundlage gemäß Art. 6 Abs. 1 DS-GVO bedarf. In Frage kommt in diesen Sachverhaltskonstellationen allenfalls die Rechtsgrundlage des Art. 6 Abs. 1 Buchstabe f) DS-GVO, wonach eine Datenverarbeitung zulässig ist, wenn diese zur Wahrung eines berechtigten Interesses des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person nicht überwiegen. Wann ein Interesse berechtigt ist, ist entsprechend der Rechtsprechung des EuGH sehr weit zu verstehen.

Man mag zuweilen ein gewisses Verständnis für die Verantwortlichen entwickeln, die sich gegen ein aus ihrer Sicht erlittenes Unrecht zur Wehr setzen wollen, die Öffentlichkeit hierüber in Kenntnis setzen/informieren wollen und in einer Internetveröffentlichung den für sie angemessenen Kommunikationskanal sehen, also ein berechtigtes Interesse erkennen.

Allerdings setzt die Vorschrift des Art. 6 Abs. 1 Buchstabe f) DS-GVO weiter voraus, dass die Datenverarbeitung der Veröffentlichung personenbezogener Daten im Internet erforderlich sein muss, um den konkreten Zweck zu erfüllen. Das heißt, es darf kein gleich geeignetes, aber milderes Mittel geben. Die Veröffentlichung im Internet muss daher überhaupt dazu geeignet sein um den beabsichtigten Zweck zu erreichen. Bei einem Interesse, die Öffentlichkeit auf Sachverhalte hinzuweisen, mag dies sicherlich noch begründbar sein, in anderen Fällen sind jedoch durchaus auch andere weniger invasive Mittel denkbar.

Schließlich ist zu prüfen, ob die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person das berechtigte Interesse des Ver-

antwortlichen überwiegen. Bei dieser Interessenabwägung in den genannten Fällen muss insbesondere einbezogen werden, dass die Veröffentlichung im Internet erfolgt und damit einer unbegrenzten Anzahl von Personen zugänglich ist, eine unbegrenzte Weiterverbreitung möglich ist und auch eine spätere Löschung nur bedingt überprüfbar ist, da der Verantwortliche eben nicht weiß wann und wie die Inhalte ggfs. von Dritten weiterverarbeitet oder gespeichert wurden.

Eine ausführliche Darstellung zu der beschriebenen 3-Stufen-Prüfung findet sich in den „Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR" des EDSA vom 8. Oktober 2024.

Im Ergebnis kann die Veröffentlichung von personenbezogenen Daten Dritter im Regelfall nicht auf die Rechtsgrundlage des berechtigten Interesses gestützt werden und erfolgt daher zumeist rechtswidrig.

Veröffentlichungen personenbezogener Daten z. B. durch Namensnennung Dritter im Internet, d. h. im Rahmen von Beiträgen in sozialen Medien, in Rezensionen oder in eigenen Internetauftritten, um den eigenen Unmut über Dritte zu artikulieren, Druck auf diese auszuüben oder sich diesen gegenüber zu wehren, sind datenschutzrechtlich regelmäßig unzulässig und können nicht auf eine tragfähige datenschutzrechtliche Rechtsgrundlage gestützt werden.

Wir haben daher in den uns vorliegenden Fällen eine Anordnung zur Löschung bzw. eine Verwarnung ausgesprochen. In Einzelfällen wird derzeit noch die Weiterverfolgung der Angelegenheit im Rahmen eines Bußgeldverfahrens geprüft.

12.2 Rechtswidrige Veröffentlichungen von Inhalten auf Online-Plattformen

Gerade wenn der Verantwortliche nicht ermittelt werden kann, kann es für die Entfernung rechtswidriger Inhalte hilfreich sein diese neben der Beschwerde bei einer Datenschutzaufsichtsbehörde dem Plattformbetreiber zu melden.

Wie auch in den vergangenen Jahren erreichten uns 2024 eine Vielzahl von Eingaben zu rechtswidrigen Veröffentlichungen von Inhalten, insbesondere von Fotos auf Online- Plattformen. In den bei uns eingegangen Sachverhalten ist davon auszugehen, dass die Veröffentlichungen rechtswidrig erfolgt sind, da keine datenschutzrechtliche Rechtsgrundlage für die Veröffentlichung ersichtlich war.

In einigen Fällen konnte der Sachverhalt von uns jedoch nicht ausermittelt werden, da der Verantwortliche für die Veröffentlichung nicht ermittelt werden konnte. Bei vielen Online- Plattformen ist es ausreichend eine eMail- Adresse und ein Pseudonym anzugeben bzw. sich einen Klarnamen auszudenken, sodass es uns und oftmals auch dem Plattformbetreiber nicht möglich ist die Identität des Nutzers herauszufinden, der die rechtswidrigen Inhalte veröffentlicht hat. Wir haben die betroffenen Personen in diesen Fällen auf die Möglichkeiten aus dem seit 17. Februar vollständig anwendbaren Digital Services Act („DSA", Gesetz über digitale Dienste vom 19.10.2022) verwiesen, um eine möglichst zeitnahe und effektive Entfernung der rechtswidrigen Inhalte zu erreichen.

Der DSA gilt neben der DS-GVO und verpflichtet Hostingdienste und Online- Plattformen unter anderem dazu, Meldeverfahren für die Meldung rechtswidriger Inhalte bereitzustellen. Die Rechtswidrigkeit ergibt sich nicht aus dem DSA selbst, sondern kann sich aus allen unionsrecht-

lichen oder mitgliedsstaatlichen Regelungen ergeben, so auch aufgrund einer Rechtswidrigkeit nach der DS-GVO. Ob der Diensteanbieter in der EU oder außerhalb niedergelassen ist, ist für die Anwendbarkeit des DSA nicht entscheidend, sondern nur ob ein Dienst innerhalb der EU angeboten wird und nutzbar ist.

Die Dienste sind dann verpflichtet, diese Meldungen zu prüfen und ggf. Maßnahmen gegen rechtswidrige Inhalte zu ergreifen. Sofern ein Dienst diesen Pflichten nicht nachkommt oder erst gar kein solches Meldeverfahren anbietet, besteht die Möglichkeit sich an den sog. Digital Services Coordinator zu wenden, dies ist in Deutschland die Bundesnetzagentur. Weiterer Informationen sind auch unter https://www.dsc.bund.de/DSC/DE/2DSA/start.html abrufbar.

12.3 Update Webtracking nach TDDDG (vormals TTDSG)

Der Anwendungsbereich des § 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ist grundsätzlich weit zu verstehen und umfasst nicht nur aktive Zugriffe und Speicherprozesse.

Wie auch in den letzten Jahren bezieht sich ein Großteil der im Bereich Internet eingehenden Beschwerden auf das Thema „Webtracking". Wie bereits in den letzten Tätigkeitsberichten (zuletzt 2023 unter 14.2 Webtracking nach dem Telekommunikations- Telemedien- Datenschutzgesetz, kurz: TTDSG) berichtet, richtet sich die Rechtmäßigkeit des Einsatzes von Tracking- Tools nicht nur nach der DS-GVO sondern auch nach Art. 5 Abs. 3 der ePrivacy- Richtlinie. Diese Norm wurde 2021 durch § 25 Telekommunikations- Telemedien- Datenschutzgesetz in das nationale Recht umgesetzt. Dieses Gesetz heißt nun seit 14. Mai 2024 Telekommunikation- Digitale- Dienste- Datenschutz- Gesetz (TDDDG). Grund hierfür ist, dass gemäß Art. 8 Änderungsgesetz zur Einführung des Digitale-Dienste-Gesetzes der Begriff „Telemedien" im TTDSG nunmehr durch den Begriff mit Rücksicht auf das Gesetz über digitale Dienste der EU (DSA, siehe auch 12.2) „digitale Dienste" ersetzt wurde. In der rechtlichen Beurteilung ändert sich hierdurch nichts, da § 25 TDDDG inhaltlich der Vorgängernorm des § 25 TTDSG entspricht.

Die Datenschutzkonferenz hat daher nun auch die „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien" ebenfalls an die neue Terminologie angepasst. Diese Anpassung wurde auch zum Anlass genommen, einige weitere Aktualisierungen vorzunehmen, um Rechtsentwicklungen seit der letzten Version 2021 abzubilden. Neben der Aufnahme einer Fußnote zum EU- U.S. Data Privacy Framework im Kapitel „Übermittlungen von personenbezogenen Daten an Drittländer" und einiger einzelner Anpassungen wird in der Einleitung auch betont, dass die Orientierungshilfe die EDSA Leitlinien „Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive" ergänzt.

Diese Leitlinien wurden am 7. Oktober 2024, nach einem Konsultationsverfahren in der Version 2.0 angenommen und geben die europäische Sichtweise auf den technischen Anwendungsbereich des Art. 5 Abs. 3 der ePrivacy-Richtlinie wieder.

Konkret geht es vor allem um die Frage, wann ein Speichern von Informationen auf der Endeinrichtung eines Endnutzers vorliegt bzw. wann ein „Zugriff" gegeben ist.

Auch in unserer täglichen Praxis ist diese Fragestellung oftmals entscheidend, insbesondere dann, wenn es um die Erfassung von zwangsläufig übermittelten Daten (z. B. der IP- Adresse oder Geräteinformationen) geht. Sofern davon ausgegangen wird, dass diese Übermittlungen in den Anwendungsbereich des Art. 5 Abs. 3 der ePrivacy- RL und damit auch § 25 TDDDG fallen ist im Regelfall von einer Einwilligungspflicht für

den Vorgang auszugehen. Demgegenüber wäre der Vorgang einzig nach den Vorgaben der DS-GVO zu bewerten, wenn dies nicht von § 25 TDDDG umfasst wäre und würde somit die Möglichkeit anderer Rechtsgrundlagen, insbesondere Art. 6 Abs. 1 Buchstabe f) DS-GVO eröffnen.

Die Guidelines gehen bei dieser Fragestellung von einem weiten Verständnis des „Zugriff"- und auch des Speicherbegriffs aus und sehen daher beispielsweise auch Tracking- Links und die Übermittlung von IP- Adressen als vom Einwilligungserfordernis der ePrivacy-Richtlinie umfasst an.

In der Vorgängerversion der OH Telemedien wurde dies nicht abschließend thematisiert, es wurde lediglich beispielshaft genannt, dass „aktives" Fingerprinting in jedem Fall in den Anwendungsbereich fällt (Rn. 24). Dieses Beispiel bleibt weiterhin auch in der aktuellen Version bestehen, jedoch zeigt der Hinweis auf die Guidelines, dass generell der weite Anwendungsbereich im Sinne einer europäisch gleichlaufenden Auslegung übernommen wird.

In der Praxis sind wir daher in allen Fällen betreffend den Einsatz von Diensten auf Webseiten und in Apps davon ausgegangen, dass der Anwendungsbereich des § 25 TDDDG eröffnet ist und daher nur in den sehr begrenzten Ausnahmenfällen des § 25 Abs. 2 TDDDG ein Entfallen der Einwilligungspflicht möglich ist.

Gerade vor diesem Hintergrund bleibt es allerdings bedauerlich, dass die EU- Kommission in ihrem aktuellen Arbeitsprogramm die bisherigen Anstrengungen zur Verabschiedung einer ePrivacy- Verordnung nunmehr endgültig aufgegeben hat, so dass bis auf Weiteres Rechtsunsicherheiten fortbestehen, ob ein solch von den europäischen Aufsichtsbehörden mehrheitlich angenommener weiter Anwendungsbereich des Art. 5 Abs. 3 ePrivacy- RL tatsächlich durch den Gesetzgeber gewollt war.

12.4 Opinion des EDSA zu „Consent-or-pay"-Modellen

Die Stellungnahme des EDSA konkretisiert den Beschluss der DSK zu „PUR- Abomodellen" im Hinblick auf große Online-Plattformen. Im Ergebnis geht der EDSA davon aus, dass solche „Consent-or-pay"-Modelle datenschutzkonform betrieben werden können, wenn die Anforderungen an eine wirksame Einwilligung erfüllt sind.

Bereits 2022 haben wir unter Kapitel 5.2 über die rechtliche Einordnung von sog. Abo- Modellen und den Beschluss der DSK berichtet. Nun hat der EDSA sich zu einem Teilbereich, dem Einsatz eines „Consent-or-pay"- Modells bei großen Onlineplattformen geäußert. Der Ausschuss hat damit den Einsatz der klassischen Variante des Abo- Modells, bei der eine Einwilligung über ein Consent-Banner eingeholt werden soll und die Möglichkeit abzulehnen darin besteht, ein kostenpflichtiges Abonnement abzuschließen, bei großen Onlineplattformen bewertet. In den Anwendungsbereich der Stellungnahme fallen damit vor allem sehr große Online- Plattformen und Gatekeeper im Sinne des Digital Services und Digital Markets Act („Gesetz über digitale Märkte" vom 14.09.2022), aber auch andere Plattformen. Entscheidend ist eine Einzelfallbetrachtung unter anderem anhand der Kriterien: Anzahl der Nutzer und Stellung des Unternehmens auf dem Markt.

Der eng gefasste Anwendungsbereich ergibt sich aus den Vorgaben des Verfahrens nach Art. 64 Abs. 2 DS-GVO. Dieses sieht vor, dass jede Aufsichtsbehörde eine Stellungnahme des EDSA beantragen kann, wenn es eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen auf mehr als einen Mitgliedsstaat geprüft haben möchte. Damit ist die Stellungnahme grundsätzlich auf die Fragestellung des Antrags begrenzt.

Am 17. Januar 2024 hat die niederländische Aufsichtsbehörde, zusammen mit der Norwegischen und der Hamburgischen Aufsichtsbehörde eine Anfrage gemäß Art. 64 Abs. 2 DS-GVO an den EDSA gestellt, mit der Frage:

> *Unter welchen Voraussetzungen können große Online-Plattformen sog. Consent- or-Pay – Modelle implementieren, sodass eine rechtswirksame Einwilligung für Datenverarbeitungen zum Zwecke der verhaltensbasierten Werbung abgegeben werden kann*.

Hintergrund hierfür war unter anderem die Entscheidung des EuGH in Sachen Bundeskartellamt (C- 252/ 21 vom 04.07.2023). Daraufhin wurde die Stellungnahme des EDSA in einer Arbeitsgruppe, an der auch das BayLDA beteiligt war, vorbereitet und am 17.04.2024 in der Plenumssitzung mehrheitlich von den Datenschutz-Aufsichtsbehörden der Mitgliedstaaten der EU angenommen. Entgegen den in Art. 65 und Art. 66 DS-GVO vorgesehenen Verfahren, welche einen verbindlichen Entschluss des EDSA herbeiführen, handelt es sich dabei um eine allgemeine Stellungnahme, welche keine bindende Entscheidung zu Einzelfällen darstellt.

Es ist daher nun Aufgabe der nationalen Aufsichtsbehörden die Stellungnahme in der Praxis entsprechend anzuwenden und wo nötig fortzuentwickeln. Innerhalb Deutschlands ergibt sich durch das Papier kein grundsätzlich neues Prüfschema, da die Stellungnahme keinen Widerspruch gegenüber dem Beschluss der DSK aus dem Jahr 2023 enthält.

Die Datenschutzkonformität eines solchen Modells hängt davon ab, ob eine rechtswirksame Einwilligung eingeholt wird bzw. überhaupt eingeholt werden kann. Die Anforderungen hierzu ergeben sich aus Art. 6 Abs. 1 Buchstabe a) DS-GVO und wurden durch die Rechtsprechung des EuGH, aber auch durch die Leitlinien des EDSA zur Einwilligung vielfach konkretisiert. Die Stellungnahme beleuchtet nun diese Anforderungen im Kontext eines solchen Modells bei großen Onlineplattformen, während der DSK-Beschluss in einem allgemeineren Kontext zu sehen ist und sich auf alle Anbieter eines „Consent-or-pay"-Modells bezieht. Die Unterscheidung ist für die Einzelfallentscheidung relevant, da zwar die Anforderungen an eine wirksame Einwilligung immer gleich sind, sich aber durch ein Ungleichgewicht der Macht beispielsweise eine andere Bewertung ergeben kann, wann eine Einwilligung als freiwillig anzusehen ist.

Gerade in den Fällen in denen bspw. große soziale Netzwerke auf das „Consent-or-pay"- Modell umstellen, stellt sich für viele Nutzer realistischerweise nicht die Frage nach dem „Verzicht", sondern nur die Entscheidung zwischen einwilligen oder bezahlen. Die soziale Notwendigkeit an der Teilhabe und der Möglichkeit diese Teilhabe zu erhalten oder fortzuführen, dürfte insoweit vielfach deutlich höheres Gewicht zugemessen werden, als im konkreten Fall datenschutzrechtlichen Risiken. Diese Besonderheit (Stichwort Lock-in-Effekt) ist ein Beispiel dafür, weshalb große Online- Plattformen besondere Herausforderungen bei der Umsetzung der Freiwilligkeitskriterien im Vergleich zu anderen Anbietern haben.

Damit große Online- Plattformen dennoch die Möglichkeit haben ein Bezahlabo als Alternative zur Einwilligung anzubieten, schlägt der EDSA die Einführung einer dritten Alternative vor, der sog. free alternative without behavioural advertising, ein Ansatz, der aus dem Digital Markets Act stammt, welcher ja sehr große Online- Plattformen reguliert.

Diese Alternative darf keine Verarbeitung zu Zwecken der Verhaltenswerbung beinhalten und kann z. B. eine Version des Plattform-Dienstes mit einer anderen Werbeform sein, bei der weniger (oder keine) personenbezogene Daten verarbeitet werden, z. B. kontextbezogene oder allgemeine Werbung oder Werbung zu Themen, die die betroffene Person aus einer Liste

von Interessenthemen ausgewählt hat. Durch das Angebot dieser dritten Alternative soll der Zwang der bei großen Online- Plattformen objektiv gesehen oftmals entstehen wird, aufgehoben werden, sodass eine freiwillige Einwilligung überhaupt möglich wird.

Die Stellungnahme des EDSA betont jedoch, dass eine solche dritte Alternative nicht rechtlich verpflichtend ist und auch bei großen Online-Plattformen keine Voraussetzung für den datenschutzkonformen Einsatz ist. Dies gilt aus unserer Sicht umso mehr bei Anbietern solcher „Consent-or-pay"- Modelle, die nicht in den Anwendungsbereich dieses Papiers fallen, also keine großen Online- Plattformen sind.

Aufgrund der Tatsache, dass die Stellungnahme sehr spezifische Fragestellungen aufgreift, bleibt noch offen, welche weiteren Anforderungen und Maßstäbe sich auf sämtliche Anbieter solcher Modelle beziehen, wie beispielsweise der Umgang mit Minderjährigen. Daher sind derzeit Leitlinien des EDSA zu den „Consent-or-pay"- Modellen in Arbeit, die sich an alle Anbieter richten sollen und noch offene Fragestellungen bzw. Unklarheiten klären sollen. Das BayLDA beteiligt sich wegen der großen Bedeutung für unsere aufsichtliche Praxis auch an diesen Leitlinien wieder als aktives Mitglied der Arbeitsgruppe.

13

Internationaler Datenverkehr

13 Internationaler Datenverkehr

13.1 Update 2024 zum EU-U.S. Data Privacy Framework

Die Europäische Kommission hat 2024 zur ersten turnusmäßigen Überprüfung des Angemessenheitsbeschlusses zum EU-U.S. Data Privacy Framework ein positives Fazit gezogen. Aus Sicht des Europäischen Datenschutzausschusses besteht aber in einigen Fragen noch Klärungsbedarf. Zudem sind die Entwicklungen in den USA durch die Europäische Kommission weiter zu verfolgen.

Im Berichtsjahr 2024 wurde erstmalig die in der DS-GVO vorgesehene Überprüfung (Art. 45 Abs. 4 DS-GVO) des Angemessenheitsbeschlusses der Europäischen Kommission zum EU-U.S. Data Privacy Framework (DPF) durchgeführt. Dieser Beschluss war zum 10. Juli 2023 in Kraft getreten. Durch ihn hatte die Europäische Kommission für einen erheblichen Teil von Übermittlungen personenbezogener Daten in die USA Rechtssicherheit geschaffen, was auch erhebliche Auswirkungen auf unsere aufsichtliche Tätigkeit im Berichtsjahr 2024 hatte. Zwischenzeitlich ist ein großer Teil der US-Unternehmen, die digitale Dienstleistungen anbieten und an die in diesem Zuge personenbezogene Daten aus der Europäischen Union übermittelt werden, nach dem DPF zertifiziert, sodass viele datenexportierende Unternehmen aus Europa nicht mehr selbst das Datenschutzniveau bei ihren US-amerikanischen Datenempfängern prüfen müssen. Vielmehr ist durch den Angemessenheitsbeschluss vom 10. Juli 2023 rechtsverbindlich festgestellt, dass bei den US-amerikanischen Unternehmen, die eine DPF-Zertifizierung besitzen, von einem angemessenen Datenschutzniveau im Sinne des europäischen Rechts ausgegangen wird.

Die Teilnahme eines US-Unternehmens am DPF wird durch Eintrag („Zertifizierung“) in eine vom US-Handelsministerium geführten und online verfügbaren Liste (https://www.dataprivacyframework.gov/list) und die Anmerkung „active“ dokumentiert.

Die erste turnusmäßige Überprüfung der Angemessenheitsentscheidung erfolgte im Jahresverlauf 2024 durch die Europäische Kommission unter Beteiligung von Vertretern des Europäischen Datenschutzausschusses (EDSA). Im Rahmen dieser Überprüfung wurde vor allem in den Blick genommen, inwieweit die im DPF vorgesehenen Strukturen und Verfahren etabliert wurden und in der Praxis funktionieren.

Kernaussage des Berichts der Europäischen Kommission ist, dass die US-amerikanischen Behörden im Überprüfungszeitraum alle im DPF vorgesehenen Strukturen und Verfahren etabliert haben, die für das effektive Funktionieren des DPF notwendig sind. Allerdings sei es noch zu früh, um bereits tragfähige Aussagen darüber treffen zu können, wie diese Strukturen und der DPF insgesamt in der Praxis funktionieren, dies könne vielmehr erst in der nächsten gemeinsamen Überprüfung erfolgen, die in rund drei Jahren vorgesehen ist. Andererseits wird man diese Aussage so verstehen, dass die Kommission jedenfalls bisher keine konkreten Anhaltspunkte dafür hat, dass der DPF nicht funktionieren würde. Denn wenn die Kommission Anlass für Zweifel am Funktionieren des DPF hätte, wäre sie rechtlich verpflichtet, diesen nachzugehen und für den Fall, dass die Zweifel sich bestätigen, den Angemessenheitsbeschluss aufzuheben.

Der EDSA hat einen eigenen Bericht zur gemeinsamen Überprüfung veröffentlicht (abrufbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/other/edpb-report-first-review-european-commission-implementing_en). Er erkennt darin an, dass die US-Seite

die Elemente des Zertifizierungsverfahrens rasch implementiert hat und zudem die Öffentlichkeit über das DPF umfangreich informiert. Allerdings betont der EDSA, dass es nur sehr wenige Beschwerden betroffener Personen aus der EU gegeben habe und es daher umso wichtiger ist, dass die zuständigen US-Behörden auch von sich aus („von Amts wegen") mehr stichprobenartige Kontrollen zur Einhaltung der DPF-Verpflichtungen bei den zertifizierten Unternehmen durchführen, da nur so ein tragfähiger Eindruck dafür gewonnen werden kann, inwieweit die im DPF geregelten Datenschutzgarantien bei den zertifizierten US-Unternehmen tatsächlich eingehalten werden. Festgehalten hat der EDSA auch, dass es vor dem Hintergrund der Existenz zweier Arten von DPF-Zertifizierung (Human Resources Data/HR Data versus Non-HR Data) immer noch kein gemeinsames Verständnis der US- und der europäischen von dem Begriff „HR Data" gibt. Der EDSA betont unter Verweis auf den Wortlaut des DFP, dass nach Ansicht der Datenschutzbehörden der EU-Mitgliedstaaten für die Übermittlung von Daten von Beschäftigten des übermittelnden Unternehmens auf US-Empfängerseite eine „HR Data"-Zertifizierung vonnöten ist. In dieser Angelegenheit laufen weitere Gespräche zwischen der US-Seite und den Vertretern der Europäischen Kommission und des EDSA mit dem Ziel der Klärung.

Wesentlicher Bestandteil des DFP sind Garantien und Standards zum Datenschutz im Zusammenhang mit möglichen Datenzugangsersuchen oder Datenzugriffen von Sicherheitsbehörden und Nachrichtendiensten auf der US-Seite. Auf US-amerikanischer Seite gab es hierzu in den letzten Jahren eine Reihe von Änderungen, die letztlich die Bedenken des Europäischen Gerichtshofs aus dessen Schrems-II-Entscheidung aus dem Jahr 2020 ausräumen sollten. So wurden die Kriterien der Erforderlichkeit und Verhältnismäßigkeit ausdrücklich als Voraussetzung für Zugriffe von Nachrichtendienste auf Daten eingeführt (vgl. dazu unseren Tätigkeitsbericht für 2023, Kap. 15.2). Der EDSA bedauert in seinem Bericht, dass im Rahmen der ersten gemeinsamen Überprüfung die praktische Umsetzung dieser Änderung noch nicht näher beleuchtet werden konnte. Einige Zweifel äußert der EDSA schließlich mit Blick auf die Änderung der Definition des Begriffs „electronic communication service provider" im US-Gesetz FISA 702, da der Kreis der hiervon umfassten Stellen, die nach dieser Vorschrift zur Datenherausgabe an US-Sicherheitsbehörden verpflichtet werden können, schwer abschätzbar sei und daher gewisse Zweifel bestehen, ob das Gesetz an dieser Stelle den aus dem europäischen Recht folgenden Anforderungen an Regelungsklarheit gerecht wird.

Die Übermittlung personenbezogener Daten in die USA ist sowohl für die Unternehmens- als auch für die aufsichtliche Praxis ein datenschutzrechtlicher Dauerbrenner. Nach drei Jahren, die aufgrund der Ungültigerklärung des „Privacy Shield" durch den EuGH von Rechtsunsicherheit geprägt waren, bewegte sich das Jahr 2024 infolge des Angemessenheitsbeschlusses zum DPF aus dem Vorjahr erstmals in ruhigerem Fahrwasser. In unserer eigenen aufsichtlichen Praxis gab es dennoch im Berichtszeitraum immer wieder Fragestellungen zum DPF, etwa zur Reichweite des Begriffs „HR Data" sowie zum Verhältnis zwischen DPF und Standarddatenschutzklauseln (zu letzterem siehe bereits unseren Tätigkeitsbericht für 2023). Angesichts dessen werden wir die Entwicklungen in der Praxis weiterhin sorgfältig beobachten. Es ist zudem vor dem Hintergrund verschiedener Ankündigungen nicht auszuschließen, dass auch der DPF ähnlich wie der Vorgänger-Angemessenheitsbeschluss dem Europäischen Gerichtshof zur Überprüfung vorgelegt werden wird. Solange der Beschluss indes in Kraft ist, können Unternehmen und andere Datenexporteure selbstverständlich ihre Übermittlungen in die USA darauf stützen, soweit der Empfänger über die passende DPF-Zertifizierung verfügt.

Die Europäische Kommission ist gesetzlich verpflichtet, die rechtlichen Rahmenbedingungen,

die sich auf den Schutz personenbezogener Daten auswirken können, in jedem Drittland, für das ein Angemessenheitsbeschluss besteht, laufend zu verfolgen. Dies gilt selbstverständlich auch für die USA. Die Europäische Kommission muss daher insbesondere die nach dem Regierungswechsel zu Jahresbeginn 2025 eingetretenen Entwicklungen rund um den sog. PCLOB (Privacy and Civil Liberties Oversight Board) sehr sorgfältig beobachten, da diesem Gremium eine wichtige Rolle im Kontext der Kontrolle der US-Nachrichtendienste zukommen. Meldungen, wonach Mitglieder dieses Gremiums möglicherweise ihrer Tätigkeit enthoben wurden, müssen daher von der Kommission kritisch geprüft und Nachbesetzungsverfahren aufmerksam verfolgt werden.

14

Technischer Datenschutz und Informationssicherheit

14 Technischer Datenschutz und Informationssicherheit

14.1 Worldcoin-Untersuchung

Ein erster Teil des hoch komplexen Verfahrens konnte nun abgeschlossen werden und hat zu verschiedenen Anordnungen im Bereich Betroffenenrechte geführt.

Wie wir in unserem letzten Tätigkeitsbericht 2023 unter Kapitel 16.2 „Worldcoin auf dem Prüfstand" berichtet haben, haben wir eine detaillierte Prüfung des unter dem Namen „Worldcoin" global bekannten, in der EU von einem in Bayern ansässigen Unternehmen datenschutzrechtlich verantworteten digitalen Dienstes eingeleitet. 2024 konnte ein erster Teil des Verfahrens abgeschlossen und erste Ergebnisse veröffentlicht werden.

Das Unternehmen World (vormals Worldcoin) entwickelt eine Technologie zur Unterscheidung zwischen Menschen und KI im digitalen Raum durch den sogenannten "Proof of Personhood". Diese Technologie soll u. a. dabei helfen, KI-Bots in sozialen Netzwerken zu erkennen. Gleichzeitig wurde eine Kryptowährung namens Worldcoin eingeführt. Nutzer erhalten nach der Registrierung mit einem Iris-Scan einen festen Betrag dieser Währung.

Die Technologie verwendet biometrische Daten aus Iris-Scans. Ein Gerät namens ORB macht hochauflösende Bilder der Iris, prüft diese auf Echtheit und wandelt sie in einen digitalen Iris-Code um. World(coin) speichert diesen Code auf Servern, um mehrfache Registrierungen zu verhindern. Nutzer bekommen eine zufällige Kennung (WorldID) in ihrer Smartphone-App, ein korrespondierender Teil wird auch in einer Blockchain gespeichert. Mit Hilfe von kryptografischen Verfahren der Klasse Zero-Knowledge-Protokolle sollen Nutzer nach der Registrierung ihre Identität als Mensch bestätigen können, ohne weitere persönliche Daten preiszugeben.

Das BayLDA hat seine Prüfung aufgrund der Komplexität der Technologie und der damit verbundenen datenschutzrechtlichen Fragen in mehrere Schritte unterteilt. Der erste Prüfschritt wurde 2024 abgeschlossen und behandelte die Bewertung zur Rechtsgrundlage, zur Löschpflicht der biometrischen Daten und zur Sicherheit der Verarbeitung.

Iris-Codes gelten als besonders schutzbedürftig, da sie eindeutig und nicht änderbar sind. Anders als Passwörter können sie bei Missbrauch nicht zurückgesetzt werden. Das BayLDA kam nach sorgfältiger Prüfung zum Ergebnis, dass Iris-Codes nach Widerruf der Einwilligung immer zu Löschen sind. Dies steht im Konflikt mit World(coin)s Ziel, eine einmalige Registrierung durch eine dauerhafte Speicherung der Iris-Codes zu gewährleisten.

Das Ergebnis des ersten Prüfschritts wurde europaweit im Kooperationsverfahren der DS-GVO abgestimmt und im Dezember 2024 an World(coin) übermittelt. Das Unternehmen hat gegen diesen Bescheid Klage eingereicht um die Grundsatzfragen, insbesondere zur Löschung und zur Sicherheit der Verarbeitung gerichtlich überprüfen zu lassen.

Im Laufe des Prüfverfahrens hat World(coin) die Speicherung der Iris-Codes technisch verändert. Diese werden nun nicht mehr zentral in einer Datenbank gespeichert, sondern mit der Technologie "Secure Multiparty Computation" (SMPC) verarbeitet. Dies ermöglicht grundsätzlich eine fragmentierte Speicherung der Iris-Codes an verschiedenen Stellen. Das BayLDA wird 2025 prüfen, ob die aktuelle Implementierung den Sicherheitsanforderungen der DS-GVO entspricht und ebenfalls, ob die von World(coin) angestrebte anonyme Speicherung bei Verwendung von SMPC eine Entbindung von der Löschverpflichtung der DS-GVO mit sich bringen kann.

14.2 Umfelddatenerfassung bei Fahrzeugen

Erfassung von Umfeldaufnahmen durch Serienfahrzeuge zu Entwicklungszwecken.

Im Herbst 2024 hat ein namhafter bayerischer Automobilhersteller gemeinsam mit anderen Herstellern desselben Konzerns aus anderen Bundesländern, mit der Umfelddatenerfassung bei Serienfahrzeugen begonnen. Dies betrifft bestimmte neue Modelle, die die technische Möglichkeit hierzu haben. Ziel dieser Verarbeitung ist die Verbesserung von Fahrerassistenzsystemen und der Entwicklung fortgeschrittener automatisierter Fahrtechnologien. In diesen Bereichen ist es nicht immer ausreichend, dass die Fahrzeuge auf reinen Teststrecken fahren, da bestimmte Fahrsituationen, bei denen die Sicherheitskomponenten auch möglichst fehlerfrei funktionieren sollten, nur „im echten Leben" auftreten. Tritt eine solche Situation ein und ein Steuergerät im Fahrzeug erkennt einen unklaren Umgebungszustand, dann kann es sein, dass videobasierte Umfeldaufnahmen in Kombination mit kurzen Standortverläufen vom Fahrzeug aufgenommen und zum Hersteller zur Analyse und Produktverbesserung übertragen werden, sollte gerade eine derartige Kampagne in der Entwicklungsabteilung laufen.

Aus Sicht des Datenschutzrechts erkennen wir durchaus ein berechtigtes Interesse von Seiten eines Autoherstellers an, wenn dieser mit derartigen Aufnahmen die Fahrsicherheit verbessern und Innovationen ermöglichen möchte. Weiterhin muss die jeweilige Datenverarbeitung auch notwendig sein, um diesen Zweck zu erreichen und im Rahmen der Interessenabwägung dürfen die Interessen, Grundfreiheiten und Grundrechte der betroffenen Personen nicht überwiegen. Im konkreten Einzelfall wurden durch wirksame technische und organisatorische Maßnahmen eine gute Pseudonymisierung von möglicherweise aufgenommenen Passanten erreicht, was sich auch positiv auf die Interessensabwägung nach Art. 6 Abs. 1 Buchstabe f) DS-GVO niedergeschlagen hat.

Anhand einer, bei derartigen Verarbeitungen gesetzlich gebotenen Datenschutzfolgenabschätzung (DSFA) nach Art. 35 DS-GVO können zudem mögliche hohe Risiken von Seiten des Verantwortlichen erkannt und vor Inbetriebnahme eingedämmt werden. Das BayLDA wird in enger Abstimmung und umfassenden Einvernehmen mit den weiteren betroffenen Datenschutzaufsichtsbehörden diese technischen Innovationsprozesse der Fahrzeughersteller mit seiner Expertise eng begleiten. Gemeinsames Ziel ist es, die Verantwortlichen frühzeitig für datenschutzrechtliche Risiken und geeignete Maßnahmen zur Gewährleistung der Betroffenenrechte zu sensibilisieren und zur Einhaltung datenschutzrechtlicher Anforderungen anzuhalten.

15

Cybersicherheitslage

15 Cybersicherheitslage

Cybersicherheitslage 2024: Hohe Bedrohungen für kleine und mittlere Unternehmen

15.1 Einführung

Die Cybersicherheitslage für kleine und mittlere Unternehmen (KMU) hat sich 2024 mit ca. 80% der Meldungen von erfolgreichen Cyberangriffen nach Art. 33 DS-GVO verschlechtert. KMU sind wohl zu Hauptzielen für Cyberkriminelle geworden, da sie oft schwächere Sicherheitsmaßnahmen als große Unternehmen haben, aber dennoch über wertvolle Daten und – in der Summe betrachtet – interessante finanzielle Ressourcen verfügen. Die fortschreitende Digitalisierung von Geschäftsprozessen hat potenzielle Angriffsflächen vergrößert, während Cyberkriminelle gleichzeitig professioneller geworden sind. Erfolgreiche Angriffe haben vielfältige Folgen, die von vorübergehenden Betriebsunterbrechungen und erheblichen finanziellen Schäden bis hin zu langfristigem Vertrauensverlust bei Kunden und Geschäftspartnern reichen.

15.2 Hauptbedrohung für KMU

1. Ransomware als existenzielle Bedrohung

Ransomware-Angriffe blieben 2024 eine ernsthafte Cyberbedrohung für KMU. Trotz internationaler Verhaftungen einiger Cyberkrimineller ist die Zahl der gemeldeten Ransomware-Angriffe bei bayerischen Unternehmen nicht nachhaltig zurückgegangen. Das "Ransomware as a Service" (RaaS)-Modell hat die Einstiegshürde für Cyberkriminelle wohl auf Dauer gesenkt und ermöglicht Angreifern ohne umfassende technische Kenntnisse, die etablierte Ransomware-Infrastruktur gegen Provision oder Festpreis zu nutzen.

Eine neue Entwicklung ist der verstärkte Einsatz spezialisierter Malware, die darauf ausgelegt ist, fortschrittliche Schutzlösungen auf Arbeitsplatzrechnern zu deaktivieren. Zusätzlich bleibt die bereits etablierte Strategie der "doppelten Erpressung" (Double Extortion) auch in 2024 als Standardvorgehensweise bestehen, obwohl auch die Variante, Daten zu stehlen ohne sie zu verschlüsseln, aus den Vorjahren fortgesetzt wurde.

2. Daten- und Identitätsdiebstahl

Neben Ransomware hat sich der gezielte Daten- und Identitätsdiebstahl verstärkt. Moderne "Stealer"-Malware und Keylogger haben sich in ihrer Funktionalität erheblich weiterentwickelt und können mittlerweile sensible Informationen wie Zugangsdaten, Kundendatenbanken und Geschäftsgeheimnisse nahezu unbemerkt abgreifen.

Angriffe auf geschäftlich genutzte E-Mail-Konten haben sich laut verschiedenen Studien wohl als besonders lukrativ erwiesen. Bei diesen Angriffen werden E-Mail-Konten von Führungskräften oder Finanzmitarbeitern kompromittiert oder überzeugend imitiert, um betrügerische Überweisungen zu veranlassen oder umfangreiche Phishing-Kampagnen innerhalb des Unternehmens zu starten. Dieses Vorgehen deckt sich auch mit einer nicht unerheblichen Anzahl an Meldungen zu erfolgreichen Betrugsversuchen bei uns in 2024.

Spear-Phishing-Angriffe, die auf Entscheidungsträger in KMU abzielen, können grundsätzlich durch KI-Technologien eine neue Qualität erreichen, obwohl KI in den Meldungen bayerischer Unternehmen bislang nicht besonders auffällig wäre. Es wird jedoch ein deutlicher Anstieg erwartet, da Cyberkriminelle durch automatisierte Sammlung und Auswertung öffentlich zugänglicher Informationen aus sozialen

Medien, Unternehmenswebsites und Branchenveranstaltungen hochpersonalisierte KI-generierte Phishing-Nachrichten erstellen können, die selbst für geschulte Mitarbeiter schwer als betrügerisch zu erkennen sind.

3. Cyberkriminalität als Dienstleistung („Cybercrime-as-a-Service")

Laut verschiedenen Studien hat sich das Geschäftsmodell "Cybercrime-as-a-Service" 2024 vollständig etabliert und zu einer hochprofessionellen Untergrundwirtschaft entwickelt. Access Broker, die sich auf den Handel mit kompromittierten Zugangsdaten spezialisiert haben, verzeichneten dabei wohl in 2024 einen Umsatzanstieg von etwa 60%, wobei Zugangsdaten zu Cloud-Diensten, Remote-Zugängen und Administrationsschnittstellen von KMU besonders gefragt waren.

Exploit-Marktplätze, auf denen Zero-Day-Schwachstellen gehandelt werden, haben sich laut verschiedenen Berichten zu einem zentralen Element der cyberkriminellen Infrastruktur entwickelt. Besonders begehrt seien dabei Schwachstellen in weit verbreiteten Business-Anwendungen und Cloud-Diensten, die von KMU genutzt werden. Sollte sich dies bei bayerischen Unternehmen, insbesondere KMU bestätigen, dann wären insbesondere die häufig erfolgreichen Angriffe auf Remote-Zugangslösungen oder Cloud-Lösungen damit zu erklären.

15.3 Praxisbericht: Wie Angriffe auf KMU ablaufen

1. Erste Infektion und Zugangsverschaffung

Der initiale Zugang zu KMU-Netzwerken erfolgt weiterhin häufig über Phishing-E-Mails mit schädlichen Links oder Anhängen. Moderne Phishing-E-Mails imitieren nicht nur perfekt das Erscheinungsbild vertrauenswürdiger Unternehmen oder Geschäftspartner, sondern sind auch inhaltlich so überzeugend gestaltet, dass selbst erfahrene Mitarbeiter getäuscht werden können. Besonders effektiv sind dabei kontextbezogene Angriffe, die aktuelle Geschäftsvorgänge oder branchenspezifische Ereignisse als Aufhänger nutzen.

Die Ausnutzung unsicherer Remote-Zugänge, insbesondere RDP (Remote Desktop Protocol) und VPN-Dienste mit schwachen Authentifizierungsmechanismen, bleibt ein zentraler Angriffsvektor. Scans nach solchen exponierten Diensten im Internet werden kontinuierlich und automatisiert durchgeführt. Laut aktuellen Statistiken werden neu eingerichtete, ungesicherte Remote-Zugänge im Durchschnitt mitunter nach 25 Minuten erstmals gescannt und auf Schwachstellen geprüft.

2. Verbreitung innerhalb des Netzwerks

Nach erfolgreicher Erstinfektion nutzen Angreifer zunehmend legitime Tools wie Fernwartungstools oder PowerShell-Skripte für die sogenannte laterale Bewegung im Netzwerk. Der Einsatz solcher legitimen Werkzeuge erschwert die Erkennung durch Sicherheitssysteme erheblich, da diese Aktivitäten kaum von normalen administrativen Tätigkeiten zu unterscheiden sind.

Die Nutzung gestohlener Zugangsdaten für Cloud-Dienste und ERP-Systeme blieb 2024 eine bevorzugte Methode zur Ausweitung der Kompromittierung. Dabei werden nicht nur lokale Netzwerke infiltriert, sondern zunehmend auch die für KMU geschäftskritischen Cloud-Infrastrukturen. Besonders problematisch könnte hierbei die vermutete weit verbreitete Praxis der Passwortwiederverwendung in KMU sein, die davon ausgehen, dass möglicherweise mehr als 60% der untersuchten KMU identische oder sehr ähnliche Passwörter für verschiedene Dienste und Systeme verwenden. Dies würde Angreifer nicht nur die Attacken über Internet, sondern auch die Übernahme interner Systeme erheblich erleichtern.

3. Exfiltration und Verschlüsselung von Daten

Im Jahr 2024 hat sich die bereits etablierte Taktik des vorgelagerten Datendiebstahls vor der eigentlichen Ransomware-Attacke als Standardvorgehensweise bestätigt. Laut Studien verbleiben Angreifer durchschnittlich bis zu 12 Tage unentdeckt in kompromittierten Netzwerken, bevor sie mit der Verschlüsselung beginnen. Diese Zeit wird genutzt, um systematisch wertvolle Informationen, einschließlich personenbezogener Daten, zu identifizieren und auf Server unter Kontrolle der Angreifer zu übertragen.

Darknet-Marktplätze fungieren mittlerweile wohl als zentrale Handelsplattformen auch für gestohlene Unternehmensdaten. Besonders gefragt seien in 2024 dabei auch Kundendaten mit persönlichen und finanziellen Informationen, geistiges Eigentum wie Konstruktionspläne oder Softwarecode sowie Geschäftsgeheimnisse wie Preiskalkulationen oder Übernahmestrategien.

Die Veröffentlichung von aus Unternehmensnetzwerken gestohlenen Daten auf speziellen Leak-Seiten bleibt auch in 2024 eine wirksame Erpressungsmethode. Die Anzahl solcher Leak-Seiten hat 2024 zugenommen, was die wachsende Professionalisierung dieser Erpressungsmethode und deren agile Anpassung an die zunehmend international ausgerichtete Strafverfolgung unterstreicht.

15.4 Fazit

Die Cybersicherheitslage für KMU hat sich 2024 weiter verschlechtert. Kleine und mittlere Unternehmen sind besonders gefährdet, da Cyberkriminelle gezielt Organisationen mit geringem Schutzniveau, aber wertvollen Daten und ausreichenden finanziellen Ressourcen für Lösegeldzahlungen ins Visier nehmen.

Ransomware, Phishing und Datendiebstahl haben sich als die prägenden Bedrohungen etabliert, wobei die Grenzen zwischen diesen Angriffsformen zunehmend verschwimmen. Die meisten Angriffskampagnen kombinieren verschiedene Techniken und Vorgehensweisen, um ihre Erfolgswahrscheinlichkeit zu maximieren. Besonders besorgniserregend ist die zunehmende Professionalisierung der Angreifer, die arbeitsteilig und mit hochentwickelten Werkzeugen operieren.

Wirksame Schutzmaßnahmen müssen auf technischer, organisatorischer und personeller Ebene ansetzen. Aus diesem Grund hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) seine Cyberpräventionstätigkeiten 2025 mit dem neuen Projekt "Cyberfestung" intensiviert. Es wird im Laufe des Jahres 2025 mehrere Möglichkeiten für bayerische KMU anbieten, ihr Cybersicherheitsniveau zu testen, und stellt entsprechende Checklisten mit technischen und organisatorischen Cyberabwehrmaßnahmen unter http://www.cyberfestung.de zur Verfügung. Eine Checkliste mit 10 besonders relevanten Schutzbereichen ist mit Erscheinen dieses Tätigkeitsberichts bereits auf der Webseite des BayLDA zum Download vorhanden.

16

Künstliche Intelligenz

16 Künstliche Intelligenz

16.1 KI datenschutzkonform einsetzen

Stellungnahme des EDSA zu KI- Modellen gibt erste Orientierung für Grundsatzfragen.

Im Laufe des Berichtszeitraums wurden wir immer häufiger mit Fragenstellungen zum Zusammenspiel der Verordnung über Künstliche Intelligenz (KI-VO) und DS-GVO und generell zum datenschutzkonformen Einsatz von KI- Modellen bzw. KI- Systemen konfrontiert. Insbesondere im Bereich Beschäftigtendatenschutz wurden verschiedene Sachverhalte an uns herangetragen, bei denen KI-Systeme zur Verarbeitung personenbezogener Daten eingesetzt wurden. Diese konnten auch vielfach mit Hilfe der Orientierungshilfe der DSK zu Künstlicher Intelligenz begleitet bzw. bearbeitet werden. Darüber hinaus ergaben sich aber generelle Fragestellungen, die bislang weder deutschlandweit noch auf europäischer Ebene einheitlich beantwortet wurden.

Umso mehr ist zu begrüßen, dass zu einem Teil dieser Grundsatzfragen nun eine Stellungnahme des EDSA, die „Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models" vorliegt. Die am 17.12.2024 verabschiedete Stellungnahme geht auf eine Anfrage der irischen Aufsichtsbehörde in einem Art. 64 Abs. 2 DS-GVO - Verfahren zurück (Ausführungen zur Verfahrensweise finden sich Im Beitrag „Opinion des EDSA zu „Consent-or-pay"- Modellen" in Kapitel 12.4).

Zusammengefasst stellt der Antrag folgende Fragen: (1) wann und wie ein KI-Modell als "anonym" angesehen werden kann; (2) wie die für die Verarbeitung Verantwortlichen die Angemessenheit des berechtigten Interesses als Rechtsgrundlage in der Entwicklungs- und (3) Einführungsphase nachweisen können; und (4) welche Folgen eine unrechtmäßige Verarbeitung personenbezogener Daten in der Entwicklungsphase eines KI-Modells auf die spätere Verarbeitung oder den Betrieb des KI-Modells hat.

Die Stellungnahme gibt den Datenschutzaufsichtsbehörden zunächst Anhaltspunkte zur Bewertung der Anonymität eines KI- Modells, betont aber, dass nicht automatisch von einer Anonymisierung auszugehen ist, nur aufgrund der Tatsache, dass personenbezogene Daten innerhalb eines KI- Modells technisch organisiert sind bzw. nicht offenkundig als personenbezogene Daten erkennbar sind. Ob die personenbezogenen Daten im KI- Modell als anonym anzusehen sind, ist anhand von Dokumentationen der ergriffenen Maßnahmen durch den Verantwortlichen im Rahmen seiner Rechenschaftspflicht entsprechend Art. 5 Abs. 2 DS-GVO darzulegen.

Sofern personenbezogene Daten verarbeitet werden, bedarf es für diese Verarbeitung auch im Rahmen von KI einer datenschutzrechtlichen Rechtsgrundlage entsprechend Art. 5 Abs. 1 i. V. m. Art. 6 DS-GVO. Hier kommt oftmals vor allem die Rechtsgrundlage des berechtigten Interesses, Art. 6 Abs. 1 Buchstabe f) DS-GVO in Betracht. Aufgrund der konkreten Fragestellung der irischen Aufsichtsbehörde sind andere Rechtsgrundlagen nicht Bestandteil der Stellungnahme, sondern diese enthält lediglich Ausführungen zu Art. 6 Abs. 1 Buchstabe f DS-GVO.

Diese enthalten eine schrittweise Erläuterung der - im Einklang mit der Rechtsprechung – und zuletzt in den Guidelines 1/2024 „on processing of personal data based on Article 6(1)(f) GDPR" ausführlich dargestellten Drei-Stufen-Prüfung im Kontext Entwicklung bzw. Einsatz eines KI-Modells. Im Ergebnis sieht es der EDSA grundsätzlich als möglich an diese Rechtsgrundlage

zu wählen, verweist jedoch darauf, dass es auf den konkreten Einzelfall ankommt und keine pauschale Aussage möglich ist.

Für die meisten Sachverhalte, die wir bisher in der Praxis zu bewerten hatten und haben werden kommt es aber wohl entscheidend auf die vierte Frage des irischen Requests an: Können rechtswidrig trainierte KI- Modelle überhaupt datenschutzkonform eingesetzt werden? Rechtswidrig trainierte Modelle meint in diesem Zusammenhang, dass das Training mit personenbezogenen Daten nicht wirksam auf eine der Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO gestützt werden kann. Im Regelfall war es bei den bisher eingegangenen Beschwerden und Beratungsanfragen so, dass beispielsweise große Sprachmodelle (Large Language Models) von bekannten Anbietern eingesetzt wurden und oftmals unklar ist, ob diese rechtmäßig trainiert worden sind. Nun stellt sich die Frage, inwiefern Einsetzende dies prüfen müssen und welche Auswirkungen der Einsatz eines solchen Modells hat.

Der EDSA trifft auch hier keine pauschale Aussage, sondern verweist zunächst einmal darauf, dass der Verantwortliche die Rechtmäßigkeit seiner Verarbeitungstätigkeiten im Rahmen der Rechenschaftspflicht gegenüber den Aufsichtsbehörden nachweisen können muss. Der Verantwortliche muss daher zunächst einmal feststellen, für welche Datenverarbeitungen er verantwortlich ist und bewerten, ob und für welche Verarbeitungstätigkeiten und in welchem Umfang beispielsweise auch eine gemeinsame Verantwortlichkeit mit dem Entwickler besteht.

Weiterhin spricht sich der EDSA dafür aus, dass die Aufsichtsbehörden berücksichtigen sollten, ob der neue Verantwortliche eine Bewertung vorgenommen und bestimmte Kriterien mit einbezogen hat. Wichtigstes Kriterium in der Praxis wird sicherlich die Feststellung der rechtswidrigen Verarbeitung in der Entwicklungsphase durch die Entscheidung einer Aufsichtsbehörde bzw. eines Gerichts sein, die im Regelfall dazu führen wird, dass eine rechtskonforme Nutzung nicht möglich ist.

Diese Feststellung muss dann in die generelle Bewertung des Verantwortlichen mit aufgenommen werden und beispielsweise bei einem Einsatz auf Grundlage des berechtigten Interesses mit in die Interessensabwägung einfließen. Es kommt daher auch hier im Ergebnis auf eine Einzelfallbetrachtung an.

Um eine einheitliche Auslegung dieses Papiers auch in der Praxis, zumindest innerhalb Deutschlands zu gewährleisten, setzt sich auch der neu gegründete Arbeitskreis KI (vormals Taskforce KI) der Datenschutzkonferenz mit bestimmten praktischen Anwendungsfällen auseinander um die Stellungnahme fortzuentwickeln.

17

Bußgeldverfahren

17 Bußgeldverfahren

17.1 Bericht aus der Zentralen Bußgeldstelle

Erneut höchste Zahl an verhängten Bußgeldern seit Geltungsbeginn der DS-GVO.

Ein Großteil der von der Zentralen Bußgeldstelle im Berichtszeitraum bearbeiteten Fälle ging erneut auf Ordnungswidrigkeitenanzeigen der Polizei zurück, jedoch konnte im Vergleich zu den Vorjahren auch ein deutlicher Anstieg an Fällen, festgestellt werden, die von den Fachbereichen an die Zentrale Bußgeldstelle abgegeben wurden..

Die starke Zunahme an Fallabgaben ist auch darauf zurückzuführen, dass im Jahr 2024 durch eine interne Schulung für die Fachbereiche und eine Neugestaltung interner Prozesse und für die Abgabe von Vorgängen relevanter Dokumente die Zusammenarbeit zwischen den Fachbereichen und der Bußgeldstelle weiter ausgebaut werden konnte. Da die letzten Schulungen und Aktualisierunsprozesse bereits einige Zeit zurücklagen, konnten schon mit diesen Maßnahmen die Abgabe festgestellter Datenschutzverstöße ins Bußgeldverfahren noch effizienter ausgestaltet werden. Neue Mitarbeiter erhielten dadurch auch die Gelegenheit, sich mit der Arbeit und den besonderen Fragestellungen der Zentralen Bußgeldstelle vertraut zu machen.

Im Berichtszeitraum wurden Bußgelder gegen Unternehmen, Freiberufler und Privatpersonen in einer niedrigen sechsstelligen Höhe verhängt, wobei nicht alle Entscheidungen bis zum Redaktionsschluss rechtskräftig wurden. Mit der höheren Anzahl an festgesetzten Bußgeldern ging gleichzeitig auch eine höhere Anzahl an Einsprüchen gegen diese Entscheidungen einher, so dass erstmalig auch mit einer größeren Zahl gerichtlicher Entscheidungen über die von dem Bayerischen Landesamt für Datenschutzaufsicht verhängten Bußgelder zu rechnen ist.

Die Spanne der festgesetzten Geldbußen reicht von Sanktionen gegen Privatpersonen in dreistelliger Höhe bis zu einer fünfstelligen Geldbuße gegen ein Kreditinstitut. Geahndet wurden im Wesentlichen unrechtmäßige Verarbeitungen, daneben aber auch Verstöße gegen Art. 5 Abs. 1 Buchstabe f), 7, 12 i. V. m. 15, 13 und 32 DS-GVO.

Besonders hervorzuheben sind zwei Einzelfälle, die im Berichtszeitraum mit erhöhten Geldbußen sanktioniert wurden:

In einem Fall legte der Betreiber eines Seniorenheims einen recht sorglosen Umgang mit Arbeitsunfähigkeitsbescheinigungen und ärztlichen Bescheinigungen über die Erkrankung minderjähriger Kinder seiner Beschäftigten an den Tag. In der Einrichtung war es üblich, Krankmeldungen in dem Stationszimmer der Station, auf der der betroffene Beschäftigte tätig war, an einer Pinnwand auszuhängen, um die Stationsleitung so über die Abwesenheit des Mitarbeitenden zu informieren. Anschließend wurden die Atteste in einem Ordner abgelegt, der sich in einem Schrank im Vorraum des Stationszimmers befand und auf den, neben der jeweiligen Stationsleitung, auch alle anderen Beschäftigten der Station Zugriff hatten. Die Praxis wurde zwischenzeitlich geändert, das Verhalten jedoch wegen eines Verstoßes gegen Art. 32 DS-GVO sanktioniert.

In einem anderen Vorgang holten Mitarbeiter mehrerer Filialen eines Kreditinstituts entgegen interner Weisungen Einwilligungen von Kunden zu Daten- und Werbeanalysen ein, in dem sie diese schriftlich aufforderten, das entsprechende Einwilligungsformular zu unterzeichnen, da anderenfalls kein vollumfänglicher Schutz ihrer Daten gewährleistet sei. Es sollte damit offensichtlich der irrtümliche Eindruck erweckt werden, die Erteilung der Einwilligungen sei für die Gewährleistung der Datensicherheit erforderlich. Das Einwilligungsformular, mit dem die

Kunden des Kreditinstituts in die Verarbeitung umfangreicher, zum Teil sensibler Daten wie beispielsweise Zahlungsverkehrsdaten, Informationen zu Konten und Kreditkarten und Daten zur Bonität, zu verschiedenen Zwecken einwilligen konnten, war bereits an allen Stellen durch die an dem Vorgang beteiligten Mitarbeiter des Kreditinstituts angekreuzt, um allein durch die Unterschrift des Kunden eine Einwilligung in die Verarbeitung zu sämtlichen Zwecken einholen zu können. Obwohl von dem Kreditinstitut verschiedene organisatorische und technische Maßnahmen ergriffen wurden, um eine datenschutzkonforme Einholung von Kundeneinwilligungen zu gewährleisten, waren diese im Ergebnis nicht ausreichend, um ein solches standortübergreifendes, weisungswidriges Handeln einzelner Mitarbeiter zu verhindern. Alle rechtswidrig eingeholten Einwilligungsformulare wurden von dem Kreditinstitut nach Bekanntwerden des Vorgangs umgehend und proaktiv gelöscht. Vermögensschäden der betroffenen Kunden sind nicht bekannt geworden. Das Kreditinstitut kooperierte sowohl im Verwaltungsverfahren als auch im Bußgeldverfahren umfassend mit dem Bayerischen Landesamt für Datenschutzaufsicht, ergriff weitere Maßnahmen, um einen datenschutzkonformen Umgang mit Kundendaten in Zukunft zu gewährleisten und räumte die Tat auch ein. Gegen das Kreditinstitut wurde im Rahmen einer Verständigung eine hohe fünfstellige Geldbuße festgesetzt.

Daneben wurden auch weiterhin Fälle sanktioniert, in denen Unternehmen auf eine Rezension eines Kunden im Internet unter Offenlegung dessen personenbezogener Daten, wie dem vollständigen Namen des Kunden, dessen Adressdaten oder auch anderer Informationen über diesen, antworteten. Um sich gegen eine aus Sicht des Unternehmens ungerechtfertigte Bewertung zur Wehr zu setzen, ist die Offenlegung solcher Informationen in aller Regel nicht erforderlich und die Verarbeitung daher unrechtmäßig.

Auch die in anderen Zusammenhängen allgemein zugängliche Veröffentlichung bestimmter personenbezogener Daten, wie der Telefonnummer oder Adressdaten, im Internet wurde, wie in den Vorjahren, mit Geldbuße sanktioniert, wenn hierfür kein Rechtfertigungsgrund bestand.

Weiterhin konsequent mit Geldbuße geahndet wurde auch 2024 der unrechtmäßige Einsatz von Ortungsgeräten, mit denen der Aufenthaltsort von anderen Personen in Erfahrung gebracht werden sollten. Hierzu erreichen uns anhaltend viele Vorgänge, bei denen am Ende aber nicht immer ermittelt werden kann, wer das Ortungsgerät angebracht hat.

Auffallend war im Berichtszeitraum eine Häufung von Fällen, in denen durch private Stellen ein „Fahndungsaufruf" durch die Veröffentlichung von Aufzeichnungen aus einer Videoüberwachung gestartet wurde.

Ein Fall betraf den Betreiber mehrerer sog. „24/7-Automaten-Shops", der in einigen seiner Ladengeschäfte über dort angebrachte Bildschirme Bilder und Videos einer Person ausstrahlte, der er die Begehung eines Diebstahls in einem seiner Ladengeschäfte vorwarf. Daneben wurden an den Fensterfronten der Ladengeschäfte „Fahndungsflyer" mit mehreren Bildern weiterer Personen, die ebenfalls des Diebstahls verdächtigt wurden, ausgehangen. Verbunden war dies jeweils mit dem Aufruf, sich mit Hinweisen zur Identifizierung dieser Personen zu melden und für entsprechende Hinweise wurde eine Belohnung ausgelobt.

In einem ähnlichen Fall wurden von dem Betreiber eines sog. „24/7-Automaten-Shops" ebenfalls „Fahndungsflyer", die zwei Personen zeigten, in seinem Ladengeschäft ausgehangen. Den abgebildeten Personen warf der Betreiber des Geschäfts Diebstahl und Sachbeschädigung vor und erbat Hinweise zur Identifizierung dieser Personen an eine dort genannte Handynummer.

In einem weiteren Fall versuchte eine Privatperson mit der Veröffentlichung einer Aufzeichnung aus einer Videokamera auf dem sozialen Netzwerk Facebook in einer öffentlichen Gruppe mit zum Tatzeitpunkt 2672 Mitgliedern, Hinweise zur Identifizierung eines Ehepaares, welches sie für den Tod eines Hundes verantwortlich machte, zu bekommen. Der „Fahndungsaufruf" war mit gravierenden Folgen für die betroffenen Personen verbunden, weil es nicht nur auf Facebook, sondern auch im „echten Leben" zu Diffamierungen und Anfeindungen gegenüber den betroffenen Personen kam. Dies geschah zudem völlig zu Unrecht, da das Ehepaar sich nur zufällig in der Nähe des Grundstücks, auf dem der Hund verstarb, aufgehalten hatte, jedoch in keiner Weise an dem Tod des Hundes beteiligt war.

Diese Form öffentlicher „Fahndungsaufrufe" durch private Stellen erachten wir für unrechtmäßig. Aufgrund der damit regelmäßig einhergehenden hohen Eingriffsintensität sanktionieren wir ein solches Vorgehen in der Regel konsequent mit Geldbuße. Zur Zulässigkeit von Videoaufnahmen in „24/7-Automaten-Shops" finden sich Ausführungen in diesem Tätigkeitsbericht in Kapitel 10.

Aufgrund der stetig hohen Anzahl von Beschwerdevorgängen im Bereich der Videoüberwachung, die den weit verbreiteten Einsatz einer solchen widerspiegeln, wurden auch unrechtmäßige Aufzeichnungen mittels Videoüberwachung im Berichtszeitraum verstärkt sanktioniert, insbesondere wenn diese mit einer umfangreichen Verarbeitung personenbezogener Daten oder Tonaufnahmen einhergehen oder in einem sensiblen Kontext stattfinden.

Dies gilt in gleicher Weise für eine nicht oder nichtvollständig erteilte Auskunft, zu der durchgehend viele Beschwerden bei uns eingehen und wegen der Bedeutung des Auskunftsrechts für die betroffenen Personen mittlerweile auch eine höhere Abgabe von Fällen an die Zentrale Bußgeldstelle erfolgt.

Abschließend ist die sich auch in den Vorjahren gezeigte gute Kooperation mit den Staatsanwaltschaften und die gute Zusammenarbeit mit den Polizeibehörden, die die Zentrale Bußgeldstelle des Bayerischen Landesamtes für Datenschutzaufsicht auch im Berichtszeitraum wieder mehrfach unterstützten, positiv und dankend hervorzuheben. Die Erfahrungen unterstreichen den Mehrwert eines stetigen Erfahrungs- und Informationsaustauschs wie ihn z. B. die Bayerische Polizei u. a. durch eine regelmäßige Einladung des BayLDA zum Datenschutz-Lehrgang ihres Fortbildungsinstituts etabliert hat. Sie ermöglicht dem Landesamt derart einen regelmäßigen Austausch mit den Ansprechpartnern der bayerischen Polizeipräsidien, in dem aktuelle Fragen der Zusammenarbeit erörtert werden.

Stichwortverzeichnis

M

N

O

P

R

S

T

U

V

W

Z

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18
91522 Ansbach

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