Bayerisches Landesamt für
Datenschutzaufsicht

15. Tätigkeitsbericht

2025

15. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht
für das Jahr 2025

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 „**Guardian of fundamental rights of the European Union, weary figure burdened by overwhelming weight, EU flag blue background with golden stars, symbolic scales of justice tilting heavily, exhausted posture with shoulders slumped, dignified yet struggling, bureaucratic documents and legislative papers cascading around, dramatic lighting emphasizing burden, pay particular attention to the blindfold, conceptual art style, photorealistic quality"

Vorgelegt im März 2026 – Michael Will, Präsident

2025 – Ein Belastungstest für die Datenschutzaufsicht

Anders als in den Vorjahren stand im Datenschutzjahr 2025 schon sehr frühzeitig im Jahresverlauf fest, welche Entwicklung die Gesamtbilanz des Jahresrückblicks prägen würde:

Der sprunghafte, alle Bereiche treffende Anstieg unserer Fallzahlen, insbesondere ein Plus an Eingaben von insgesamt 61%, mithin ein Allzeithoch von knapp unter 10.000 Vorgängen, gefolgt von einem nicht minder bedeutsamen Anstieg der Meldungen von Datenschutzverletzungen von immerhin 23%.

Gleichzeitig ist die Zahl der schon zuletzt rückläufigen Beratungsanfragen auf ein Allzeittief gesunken.

Der „Guardian of a Fundamental Right", die vom EuGH schon 2010 gewählte Metapher für die Aufgaben der Datenschutzaufsichtsbehörden und ihres Schutzauftrags aus Art. 8 der EU-Grundrechtecharta vermittelt den Leserinnen und Lesern unseres 15. Tätigkeitsberichts deshalb ein zwar konzentriertes, aber doch gebeugtes, mit hohen Lasten ringendes Bild.

Hohe Beschwerdezahlen – keine Erfolgsmeldung?

Sollten hohe Beschwerdezahlen nicht aber eigentlich als Erfolgsmeldung des Datenschutzjahrs 2025 betrachtet werden? Immerhin rund zwei Drittel der rund 10.000 Eingänge des Jahres 2025 waren nach genauerer Prüfung als formale Beschwerden im Sinne von Art. 77 DS-GVO zu bewerten. Sie könnten damit auf ersten Blick als Zeugnis hoher Datenschutz-Sensibilität der betroffenen Personen Grund zum Jubel über Fortschritte beim Datenschutz geben, während doch sonst – wie noch im 14. Tätigkeitsbericht ausführlich beschrieben - die allgemeine Wahrnehmung eher einen Bedeutungsverlust signalisiert. Zum Vergleich: noch im Jahr 2015 versuchte unsere Behörde mit maßvollem Erfolg Betroffene per Zeitungsannonce zur Wahrnehmung ihres datenschutzrechtlichen Auskunftsanspruchs anzuspornen. Immerhin konnten wir dadurch vor rund einem Jahrzehnt bayernweite 31 Teilnehmende so weit motivieren, dass auf Grund ihrer Auskunftsbegehren 188 Verantwortliche proaktiv von Amts wegen geprüft werden konnten (s. 7. Tätigkeitsbericht, Ziff. 3.4).

Darf es insoweit nicht als Erfolg gewertet werden, dass in nahezu allen Fachbereichen Beschwerden im Kontext des Auskunftsrechts nach Art. 15 DS-GVO zu den Spitzenreitern der Verstöße zählen? Bedingt im Übrigen die Entwicklung zu einer digitalen Gesellschaft mit alltäglicher und allgegenwärtiger Verarbeitung personenbezogener Daten nicht nahezu zwingend, dass die Zahl der hieran anknüpfenden Beschwerden wegen vermuteter Datenschutzverstöße ansteigt?

Die vom EuGH bereits vor sechzehn Jahren zur damaligen EG-Datenschutz-Richtlinie in seiner Entscheidung vom 09. März 2010 getroffene, unter Geltung der DS-GVO unverändert gültige Aufgabenbeschreibung der Datenschutzaufsichtsbehörden würde eine solche positive Betrachtung durchaus stützen.

> „Die in Art. 28 der Richtlinie 95/46 vorgesehenen Kontrollstellen sind somit die Hüter dieser Grundrechte und Grundfreiheiten, und ihre Einrichtung in den Mitgliedstaaten gilt, wie es im 62. Erwägungsgrund der Richtlinie heißt, als ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten.
>
> Um diesen Schutz zu gewährleisten, müssen die Kontrollstellen zum einen die Achtung des Grundrechts auf Privatsphäre und zum anderen

die Interessen, die den freien Verkehr personenbezogener Daten verlangen, miteinander ins Gleichgewicht bringen. (…)" [EuGH, Urt. v. 9. 3.2010, Rs. C-518/07, Rn. 23, 24].

Eine nicht alleine quantitative Betrachtung unserer Beschwerdeeingänge des Jahres 2025 ergibt allerdings ein Bild, dass eine differenzierte Beurteilung verlangt: in einer zunehmenden Zahl an Fällen steht nicht mehr der „Schutz der Personen bei der Verarbeitung personenbezogener Daten" im Mittelpunkt, sondern klar erkennbar anderweitige Anliegen, die oft bereits Gegenstand paralleler behördlicher oder gerichtlicher Verfahren sind.

Instrumentalisierung des Datenschutzrechts

Solche Anliegen wie z. B. die Berichtigung eines Versicherungsgutachtens über die Feststellung von Berufsunfähigkeit oder der Löschung von bestimmten Zeugnissen Dritter im Rahmen eines Sorgerechts- oder Kündigungsschutzstreits betreffen nur vordergründig die eigentliche Datenverarbeitung von Versicherungen, Gutachtern oder Arbeitgebern. Sie sind deshalb aber gleichwohl im Einklang mit der Rechtsprechung des EuGH derzeit legitime, aufsichtlich kontrollier- und durchsetzbare Grundlage datenschutzrechtliche Betroffenenrechte wie etwa eines Auskunftsanspruchs.

Ist die Zunahme von Beschwerden, in denen die Datenverarbeitung nicht im Mittelpunkt des individuellen Rechtsschutzbegehrens steht, sondern nur ihren formalen Anknüpfungspunkt bildet, tatsächlich ein Erfolg für den Schutz personenbezogener Daten und Ausdruck eines hohes Schutzniveaus? Eine zunehmende Zahl dieser Beschwerden beruht erkennbar auf Empfehlungen von KI-Tools, die in einer durchaus treffsicheren Analyse verfügbarer Rechtsschutzinstrumente die Datenschutzbeschwerde als weiteres niederschwelliges, für Betroffene kostenfreies behördliches Prüfverfahren identifiziert haben.

Nach unseren Praxiserfahrungen ergeben sich gerade aus solchen hybriden Fallgestaltungen, in denen Datenschutzfragen nicht das Kernanliegen der Beschwerdeführenden darstellen, überproportional häufig ressourcenintensive Folgestreitigkeiten in Form von Gegenvorstellungen, Dienstaufsichtsbeschwerden oder gar verwaltungsgerichtlichen Klageverfahren, im Einzelfall zunehmend begleitet von Verunglimpfungen der Behörde und ihrer Handelnden im Internet bis hin zur Androhung persönlicher Nachstellungen.

Solche Reaktionen sind in vielen Fällen Ausdruck enttäuschter Erwartungen der Betroffenen auf Grund von Fehlvorstellungen über das Erreichbare. In einer nicht unbedeutenden Zahl an Fällen sind sie aber offenkundig auch Teil einer Strategie individueller Rechtsdurchsetzung, in der Datenschutz instrumentalisiert wird, um den – im datenschutzaufsichtlichen Verfahren anders als im Zivilprozess mitwirkungspflichten – Verantwortlichen zu Zugeständnissen zu veranlassen. Eine Befriedungswirkung oder gar die Erfüllung des primären Auftrags der Datenschutzaufsicht, die unionsweite Durchsetzung der DS-GVO zum Schutz der Rechte der betroffenen Person, ist in solchen Fällen, in denen das Recht auf Datenschutz bestenfalls als Eskalationsgrundrecht missbraucht wird, eigentlich von vornherein weder erreichbar noch bezweckt.

Rechtspolitische Gegensteuerung

Die aufgezeigten Entwicklungen sind für sich genommen zunächst nur Ausdruck von Fehlanreizen eines an sich angemessenen und funktionsfähigen datenschutzrechtlichen Rechtsschutzsystems. Angesichts der explosionsartigen Entwicklung der Fallzahlen nicht nur für die bayerische Datenschutzaufsicht sondern auch bei den übrigen deutschen und europäischen Datenschutzbehörden sind indessen rasche Analysen geboten und Überlegungen auch zu strukturellen Anpassungen zumindest legitim:

Hierzu zählen zunächst vor allem die Vorschläge der EU-Kommission im Rahmen des sog. Digital-Omnibus, durch Modifizierungen der schon heute bestehenden Missbrauchsklausel der DS-GVO die Inanspruchnahme der Datenschutzaufsicht zumindest wegen Verletzungen von Art. 15 DS-GVO für erkennbar datenschutzfremde Zwecke zu begrenzen (COM-Dok. 2025/0360 (COD) vom 19.11.2025, Art. 3 Nr. 4).

Angesichts begrenzter Haushaltsspielräume des Freistaats, wie auch der übrigen Länder und Mitgliedsstaaten, sollten indessen weiterreichende Maßnahmen zur Effektuierung der Datenschutzaufsicht nicht ausgeschlossen werden. Denkbare Maßnahmen wären aus hiesiger Sicht eine verwaltungsrechtliche Kostenpflicht auch für Betroffenenbeschwerden in Missbrauchsfällen, der Ausschluss paralleler Inanspruchnahme von gerichtlichem und aufsichtlichem Rechtsschutz oder die Einführung eines auch in der Strafprozessordnung gängigen Opportunitätsprinzips. Insbesondere letzteres würde anders als heute den Aufsichtsbehörden im Interesse einer risikoorientierten Steuerung ihres Handelns Spielräume eröffnen, ob und in welchen Fällen sie im Einzelfall ihrer Aufgabe als Hüter des Grundrechts auf Datenschutz am wirksamsten nachkommen können und gleichzeitig erlauben, die begrenzten staatlichen Ressourcen zur Durchsetzung individueller Datenschutzansprüche fair und effektiv zu verteilen.

Effektiverer Datenschutz durch Umverteilung aufsichtlicher Zuständigkeiten?

Parallel zur Belastungsprobe unserer Kapazitäten durch ansteigende Fallzahlen hat unsere Behörde im Jahr 2025 eine Debatte um die künftige Verteilung von Aufsichtszuständigkeiten zwischen Bund und Ländern begleitet. Zwar sind konkrete und praktikable Modelle zur Umsetzung dieses Ziels des Koalitionsvertrags der Bundesregierung bis heute nicht erkennbar geworden. Auf Grundlage der Besprechung des Bundeskanzlers mit den Regierungsschefinnen und Regierungschefs der Länder am 04.12.2025 ist bislang zumindest aber zu erwarten, dass der Bund in Abstimmung mit den Ländern die Datenschutzaufsicht für den nicht-öffentlichen Bereich bis spätestens 31.12.2027 reformieren wird. Wir werden das Datenschutzjahr 2026 deshalb dazu nutzen, die Vorzüge und Potentiale föderaler Datenschutzaufsicht aufzuzeigen und so für ihren Fortbestand über ihr im Jahr 2027 anstehendes 25-jähriges Jubiläum hinaus zu werben.

Ansbach, im März 2026

Michael Will
Präsident

Inhaltsverzeichnis

2025 – Ein Belastungstest für die Datenschutzaufsicht 1
Inhaltsverzeichnis 4
1 Datenschutzaufsicht im nicht-öffentlichen Bereich 7
1.1 Gesetzliche Grundlage für den Tätigkeitsbericht 7
1.2 Datenschutz in Bayern 7
1.3 Neue Spezialzuständigkeiten 7
1.4 Das Bayerische Landesamt für Datenschutzaufsicht 8
2 Zahlen und Fakten 10
2.1 Beschwerden 10
2.2 Beratungen 13
2.3 Datenschutzverletzungen 14
3 Europäische Zusammenarbeit 16
3.1 Verfahren der Zusammenarbeit und Kohärenz 16
3.2 Die neue EU-Verfahrensverordnung 16
3.3 Mitwirkung in Subgroups des EDSA 18
4 Allgemeines 21
4.1 Löschung der E-Mail-Adresse aus der „AutoVervollständigen-Liste" von Microsoft Outlook 21
4.2 Durchsetzung der DS-GVO in der Praxis 21
5 Datenschutzbeauftragte 25
5.1 Bereitstellung einer separaten Kontaktmöglichkeit zu Datenschutzbeauftragten (DSB) 25
6 Finanzwirtschaft 27
6.1 Beschwerden zu Forderungsstreitigkeiten 27
6.2 Bonitätsabfragen durch Inkassodienstleister vor erster Kontaktaufnahme 28
6.3 Unzureichende Löschprozesse nach dem Zusammenschluss zweier Kreditinstitute 28
7 Werbung 31
7.1 Anforderungen an den Nachweis einer wirksamen Einwilligung für Direktwerbung 31
8 Industrie und Handel, Wohnungswirtschaft 34
8.1 Personalausweise – Kopie und Pfand mit hohem Missbrauchsrisiko 34
8.2 Auch Privatpersonen können zum Verantwortlichen werden 36
8.3 Rauchwarnmelder mit Raum- und Klimamonitoring 37
9 Beschäftigtendatenschutz 40
9.1 Veröffentlichung personenbezogener Daten des Geschäftsführers im Handelsregister 40
9.2 E-Mail-Postfächer ehemaliger Beschäftigter 41
9.3 GPS-Tracking in Firmenfahrzeugen 42

10 Videoüberwachung 47
10.1 Datenschutzrechtliche Anforderung beim Einsatz sog. Dashcams 47
11 Gesundheit und Soziales, Versicherungen 50
11.1 Online-Terminbuchungen und Terminmanagement in einer Arztpraxis 50
11.2 Löschpflicht von Gesundheitsdaten bei erfolgtem Widerruf der Einwilligung 51
12 Rechtsanwältinnen und Rechtsanwälte 53
12.1 E-Mail-Kommunikation zwischen Berufsgeheimnisträgern und betroffenen Personen 53
13 Digitalwirtschaft 56
13.1 Transkription von Videokonferenzen 56
13.2 Kein Anspruch auf Freischaltung eines gesperrten Online-Accounts nach Art. 15 DS-GVO 57
13.3 Entscheidungen zum Auskunftsrecht im Onlinehandel 58
13.4 Geltungsbeginn des DataAct 60
13.5 Political Targeting 61
14 Internationaler Datenverkehr 64
14.1 Beratungsanfragen zum EU-U.S. Data Privacy Framework 64
14.2 Datenübermittlung durch Tiktok nach China 65
15 Technischer Datenschutz und Informationssicherheit 70
15.1 Cyberfestung 70
15.2 Ransomware 71
15.3 E-Mail-Account-Hacking und Phishing 72
16 Bußgeldverfahren 76
16.1 Bericht aus der Zentralen Bußgeldstelle 76
Stichwortverzeichnis 79

1

Datenschutzaufsicht im nicht-öffentlichen Bereich

1 Datenschutzaufsicht im nicht-öffentlichen Bereich

1.1 Gesetzliche Grundlage für den Tätigkeitsbericht

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

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

1.2 Datenschutz in Bayern

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

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

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

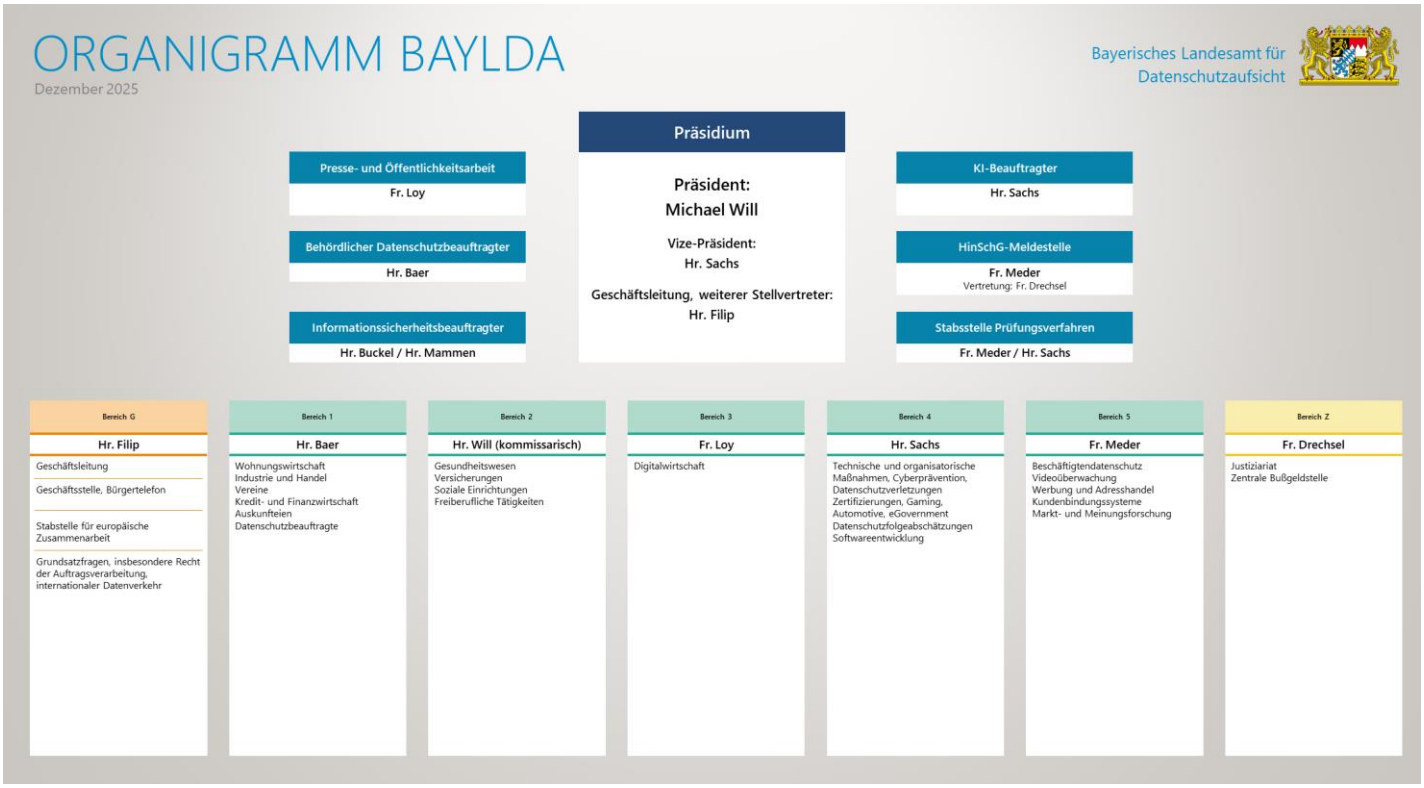
Darüber hinaus haben Kirchen, religiöse Vereinigungen oder Gemeinschaften gemäß Art. 91 DS-GVO unter bestimmten Voraussetzungen die Möglichkeit eine spezifische Aufsichtsbehörde einzurichten, die dann als Aufsichtsbehörde anzusehen ist, wenn sie die in Art. 51 ff. DS-GVO genannten Voraussetzungen, insbesondere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

1.3 Neue Spezialzuständigkeiten

Im Jahr 2025 hat das Bayerische Landesamt für Datenschutzaufsicht durch den europäischen Gesetzgeber noch zwei weitere Zuständigkeiten erhalten. Zum einen durch den Geltungsbeginn der „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung", kurz die „Daten-Verordnung" bzw. dem Data Act (Art. 37 Abs. 3 DA) und zum anderen durch die „Verordnung über die Transparenz und das Targeting politischer Werbung" (TTPW-VO) welche seit dem 10. Oktober 2025 EU-weit verbindlich anzuwenden ist (Art. 22 Abs. 1 TTPW-VO). Beide Bereiche sind dem Bereich Digitalwirtschaft des BayLDA zugeordnet, daher finden sich weitergehende Informationen hierzu in Kapitel 13.

1.4 Das Bayerische Landesamt für Datenschutzaufsicht

Die Personalausstattung des BayLDA im Berichtszeitraum belief sich auf nominell 43 Planstellen. Wie bereits im Tätigkeitsbericht 2024 unter Kapitel 1.3 dargestellt, ergibt sich dieser Zuwachs von 5 weiteren Planstellen aus dem Doppelhaushalt 2024/2025, der insgesamt 10 neue Planstellen ausgebracht hat, von denen wir 9 bis Jahresende 2025 besetzen bzw. zumindest vergeben konnten. Dank dieser Verstärkungen ist das Landesamt – unbeschadet kurzfristiger, nur mit Zeitversatz nachzubesetzender Rotationen - erstmals seit 2020 so aufgestellt, dass in allen Bereichen eine interne und nicht lediglich eine horizontale, bereichsübergreifende Vertretung gesichert ist. Der zum Redaktionsschluss noch nicht verabschiedete Entwurf des Doppelhaushalts 2026/27 sieht entgegen unseren wie in den Vorjahren schon im Hinblick auf offenkundige Aufgabenmehrungen angemeldeten Personalbedarfe keine weitere Aufstockung der Personalressourcen vor. Er enthält zudem enger gefasste Sachmittelansätze, die unsere Handlungsspielräume z. B. im Bereich der Fortbildungs- und Reisekosten auch angesichts der allgemeinen Teuerungsrate eng begrenzen. Gerade für unsere inner-deutschen wie europäischen Kooperationsaufgaben, die dem allseitigen Ziel einer kohärenten DS-GVO-Anwendung dienen, sowie insbesondere im Hinblick auf die Vorbereitung des bayerischen DSK-Vorsitzes im Jahr 2027 zeichnen sich hierdurch bereits jetzt erhebliche Herausforderungen ab.



2

Zahlen und Fakten

2 Zahlen und Fakten

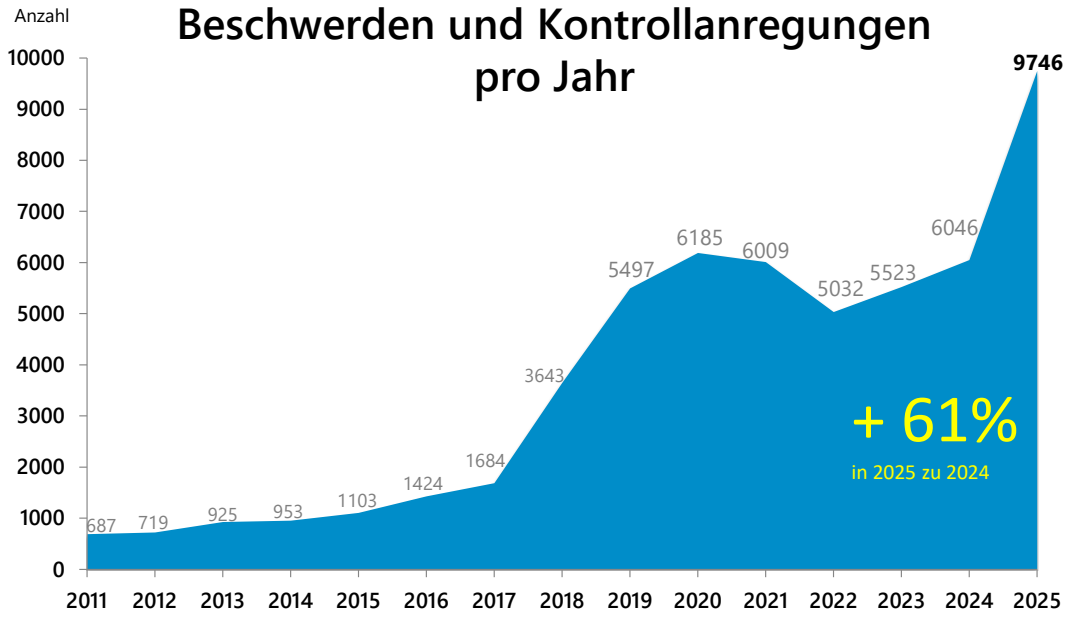
Das Jahr 2025 war für das BayLDA von einer erheblichen Zunahme der Fallzahlen geprägt. Neben der immer weiter steigenden Sensibilisierung von Bürgerinnen und Bürgern für Ihre Datenschutzrechte und neuen datenintensiven Geschäftsmodellen, ist sicherlich auch die zügige Verbreitung von Künstlicher Intelligenz (KI) und speziell von Large Language Modells (LLMs) für den Anstieg maßgeblich. Nicht jedoch aufgrund der datenschutzrechtlichen Fragestellungen in diesem Zusammenhang, sondern aufgrund der Nutzung von KI zur Erstellung von Beschwerden.

Die Hürden eine datenschutzrechtliche Beschwerde einzureichen, sind durch die Verfügbarkeit von KI- Tools noch einmal beträchtlich gesunken. Während man bislang zumindest eine gewissen Anstrengung aufbringen musste, um eine schriftliche Beschwerde zu formulieren oder unser Online- Beschwerdeformular auszufüllen, nutzen viele Betroffene nun LLMs um den Sachverhalt darzustellen und ein Anschreiben an uns zu erstellen. Diese grundsätzlich erfreuliche Tatsache, dass nun betroffene Personen eine einfache Möglichkeit haben, hat allerdings auch Schattenseiten: Oftmals werden uns nur die Chatverläufe der Gespräche mit dem Sprachmodell weitergeleitet oder Sachverhalte ganz allgemein dargestellt, indem von der KI erzeugte Platzhalter nicht befüllt werden oder die KI erfindet schlicht und einfach zusätzliche Details, die mangels Überprüfung dann so an uns weitergegeben werden. Dies führt oftmals zu Unklarheiten und dadurch zu unnötigen Ressourcenverbrauch und länger andauernden Verfahren. Wir appellieren daher an betroffene Personen KI- generierte Eingaben nicht ungesehen und ungeprüft an uns zu übermitteln.

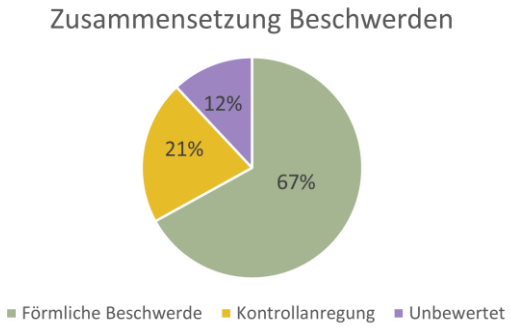
2.1 Beschwerden

Im Jahr 2025 erreichten das BayLDA insgesamt 9746 Beschwerden und Kontrollanregungen. Gegenüber dem Vorjahr stellt dies einen Anstieg um 61 % dar. Damit verzeichnen wir den höchsten Stand seit Geltungsbeginn der DS-GVO. Der bereits in den Vorjahren erkennbare Aufwärtstrend hat sich damit nochmals deutlich beschleunigt.

Von den insgesamt 9746 Eingängen entfielen 67 % auf förmliche Beschwerden und 21 % auf Kontrollanregungen. Die Übrigen 12 % stellen



noch nicht bewertete Eingänge dar, die wir zum Jahresende erhalten haben.



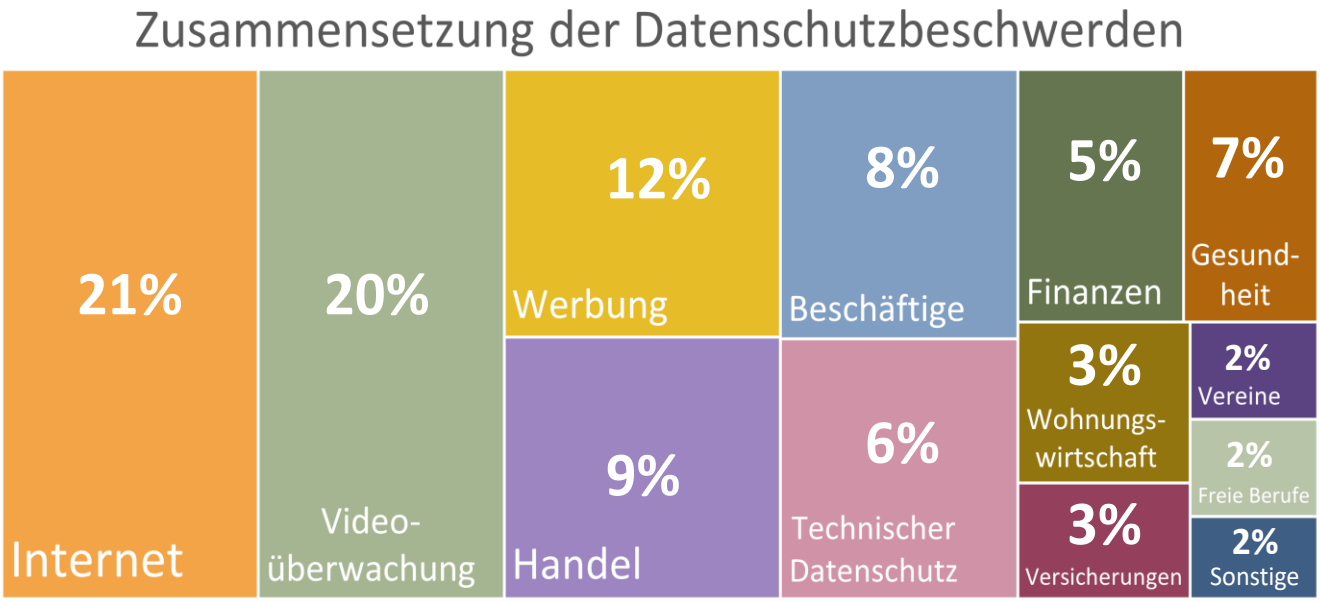
Als Beschwerden werden dabei nach wie vor solche Vorgänge gezählt, die schriftlich eingehen und bei denen eine natürliche Person eine persönliche Betroffenheit darlegt, für die Art. 78 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische „Beschwerden" werden dann gezählt, wenn sie z. B. durch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

Darüber hinaus haben wir auch weiterhin eine hohe Zahl an Eingaben, ohne eigene Betroffenheit, welche ebenfalls ein wichtiger Bestandteil unserer aufsichtlichen Tätigkeit sind. Kontrollanregungen geben oftmals Hinweise für strukturelle Probleme in einzelnen Branchen oder auch branchenübergreifend und zeigen uns stellenweise auch in welchen Bereichen Handlungsbedarf, durch Beratungen oder Prüfungen erforderlich ist.

Eine Vielzahl dieser Kontrollanregungen wurde von uns im Rahmen von amtswegigen Verfahren aufgegriffen oder teilweise auch in die generelle Prüfstrategie unserer Behörde, auch mit Blick auf zukünftige Prüfungen, miteinbezogen.

Beim Blick auf die Verteilung der Beschwerden zeigt sich, dass den größten Anteil Beschwerden der Bereich Internet und digitale Dienste (21 %) einnimmt. Hierzu zählen zwischenzeitlich vor allem Sachverhalte rund um Betroffenenrechte im Online- Bereich, aber auch weiterhin Beschwerden zum Einsatz von Tracking-Technologien und Social-Media-Dienste.

Wie auch in den vorhergehenden Jahren folgt nahezu gleichauf der Bereich Videoüberwachung (20 %). Hier bilden vor allem Beschwerden im privaten Bereich, gerade im nachbarschaftlichen Kontext, den Schwerpunkt. Generell geht es meistens darum zu überprüfen, welche Bereiche von Videokameras erfasst werden dürfen.



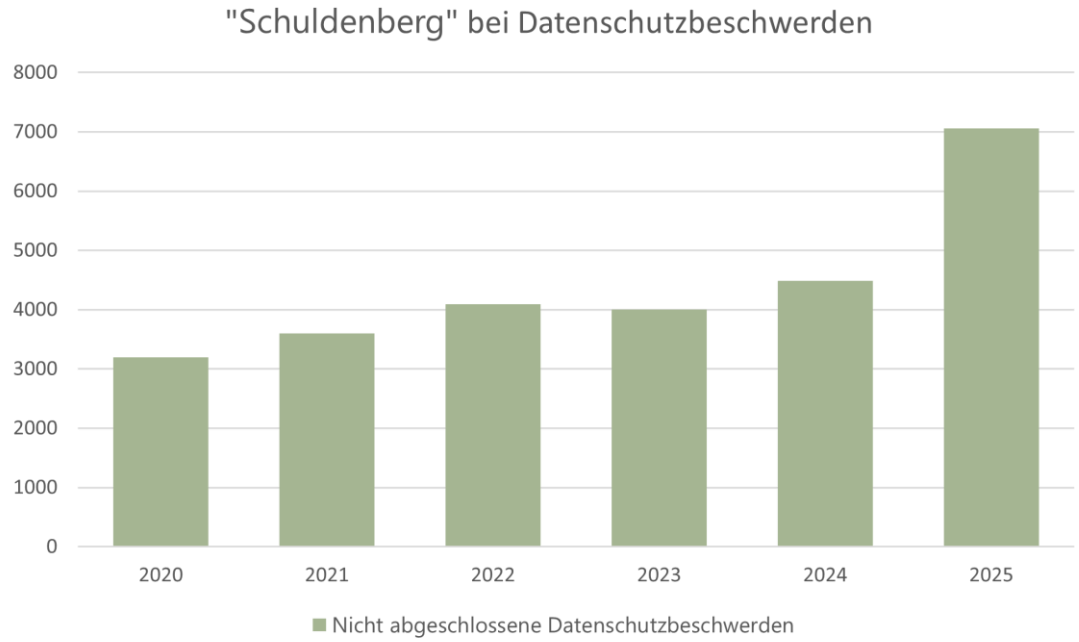
Auch ansonsten, bleibt die Verteilung im Vergleich zu den Vorjahren relativ konstant, lediglich die Bereiche Beschäftigtendatenschutz und Gesundheit zeigen einen größeren Anstieg, um jeweils 2% gegenüber dem Vorjahr.

Ein zentrales Qualitätskriterium aufsichtlicher Tätigkeit ist die Verfahrensdauer. Für das Jahr 2025 ergibt sich bei den abgeschlossenen förmlichen Beschwerden folgendes Bild: 62 % aller im Jahr 2025 abgeschlossenen förmlichen Beschwerden konnten, trotz des enormen Anstiegs der Fallzahlen, innerhalb von drei Monaten abschließend bearbeitet werden.

Die Auswertung zeigt dabei Unterschiede je nach Verfahrensart und Komplexität. Insbesondere Sachverhalte mit mehreren Beteiligten, umfangreichen technischen Prüfungen oder grenzüberschreitenden Abstimmungen führen regelmäßig zu längeren Bearbeitungszeiten.

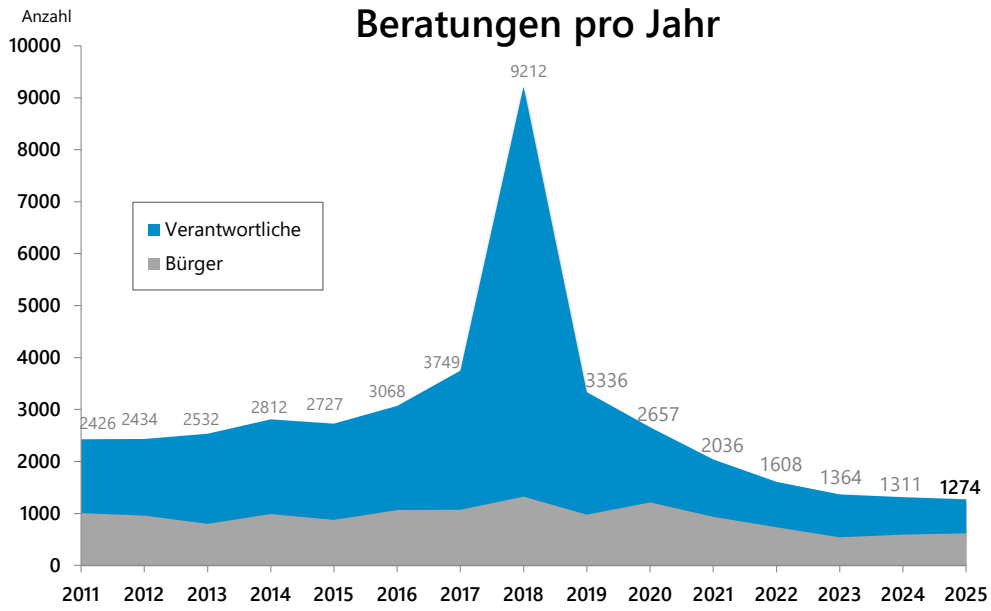
Die Entwicklung im Jahresverlauf verdeutlicht zudem einen kontinuierlichen ansteigenden Bestand offener Verfahren („Schuldenberg"). Trotz erheblicher Anstrengungen zur Verfahrensbeschleunigung wuchs der Bestand unerledigter Beschwerden im Laufe des Jahres 2025 weiter an.

Damit verdeutlichen die Zahlen insgesamt die zunehmende strukturelle Belastung der Behörde.



2.2 Beratungen

Neben Beschwerden spielt die Beratung von Verantwortlichen, betrieblichen Datenschutzbeauftragten und Betroffenen eine zentrale Rolle. Im Jahr 2025 wurden 1274 schriftliche Beratungsanfragen (aufgeteilt in Bürgerberatungen 614 und Unternehmensberatungen 660) bearbeitet. Dies stellt ein Allzeittief der Beratungen dar, welches spiegelbildlich zu den Beschwerdezahlen ist. Die Beratungstätigkeit muss angesichts begrenzter Ressourcen einer klaren Priorisierung unterliegen. Hierbei werden, wie bereits im Vorjahr dargestellt vor allem die Bereiche Cyberprävention und KI aufgrund des akuten Bedarfs weiterhin vorrangig bearbeitet.

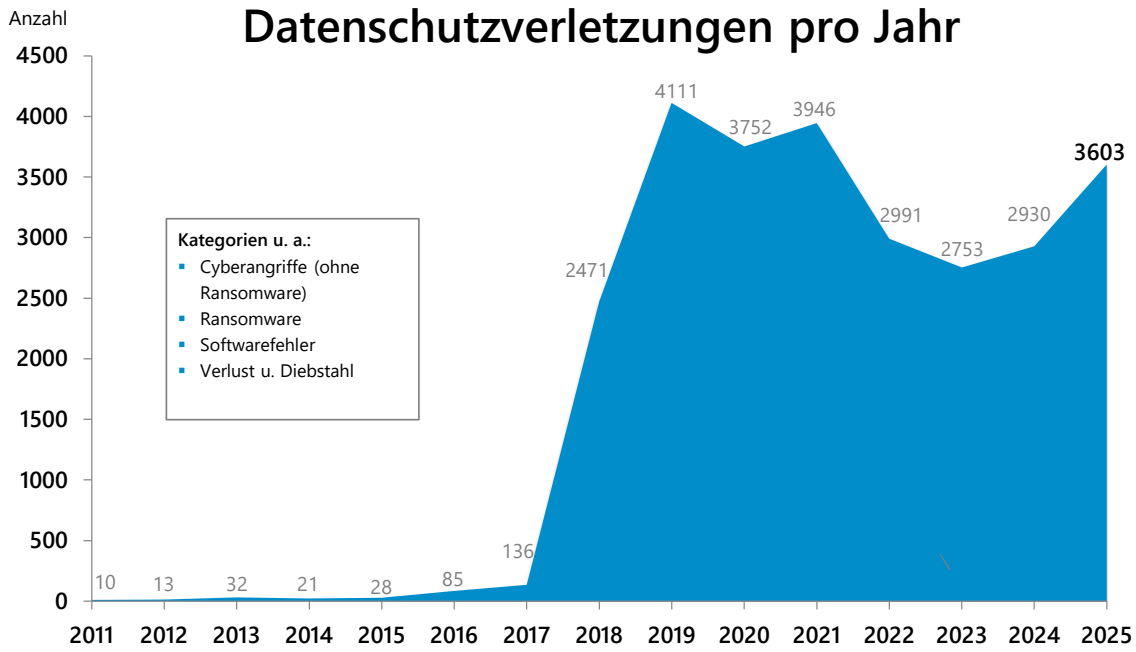


2.3 Datenschutzverletzungen

Im Jahr 2025 gingen beim BayLDA 3603 Datenpannenmeldungen ein. Damit liegt im Vergleich zum Vorjahr wieder eine Steigerung der Zahlen vor, insgesamt um 23%. Dies stellt allerdings aufgrund der hohen Bedrohungslage leider keine Überraschung dar.

Datenschutzverletzungen betreffen insbesondere:

- Cyberangriffe
- Ransomware-Fälle,
- Softwarefehler,
- Verlust und Diebstahl.



3

Europäische Zusammenarbeit

3 Europäische Zusammenarbeit

3.1 Verfahren der Zusammenarbeit und Kohärenz

Weiter steigende Zahl an Kooperationsverfahren bei anhaltend langen Verfahrensdauern.

Auch im Jahr 2025 war unser Haus an zahlreichen Beschwerdeverfahren beteiligt, die in dem von der DS-GVO vorgesehenen Kooperationsverfahren bearbeitet wurden. Insgesamt handelte es sich um 704 Kooperationsverfahren, von denen 101 im Laufe des Jahres 2025 abgeschlossen wurden und 603 zu Jahresende noch andauerten. Bei 162 dieser Kooperationsverfahren handelt es sich um solche, die im Laufe des Jahres 2025 begonnen wurden; hiervon waren wir bei 18 Verfahren EU-weit federführende Aufsichtsbehörde. Vier Kooperationsverfahren, bei denen wir die Rolle als EU-weit federführende Aufsichtsbehörde hatten, haben wir im Berichtszeitraum abgeschlossen.

Insgesamt ist zu beobachten, dass die Gesamtzahl der Kooperationsverfahren, an denen unser Haus beteiligt war, gegenüber dem Vorjahr auf ohnehin bereits hohem Niveau weiter angestiegen ist. Die Verfahren besaßen, wie auch rein national geführte Verfahren, unterschiedliche Komplexität; jedenfalls bei einem Teil der Verfahren waren aber anspruchsvolle technische und/oder rechtliche Fragestellungen zu behandeln, was tendenziell zu einer Erhöhung der Verfahrensdauer führt. Die bereits verabschiedete und ab dem 2. April 2027 geltende Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 („DSGVO-Verfahrensverordnung“) wird vor diesem Hintergrund für die Aufsichtsbehörden bei der Bearbeitung von Beschwerden, die dem Kooperationsverfahren unterliegen, mit den darin geregelten sehr engen Verfahrensfristen erhebliche Herausforderungen mit sich bringen (vgl. dazu Kapitel 3.2).

3.2 Die neue EU-Verfahrensverordnung

Die neuen Verfahrensregelungen für grenzüberschreitende Sachverhalte werden das Ressourcenproblem der Aufsichtsbehörden noch verstärken.

Die DS-GVO wird gemeinsam von den Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten in ihrem jeweiligen Zuständigkeitsbereich vollzogen. Zahlreiche Verarbeitungen personenbezogener Daten haben darüber hinaus einen sog. grenzüberschreitenden Charakter, weil sie – etwas vereinfacht gesprochen – in gleicher Weise in mehreren oder gar allen Mitgliedstaaten stattfinden. Für die Aufsicht über grenzüberschreitende Verarbeitungen sieht die DS-GVO schon seit ihrem Geltungsbeginn eine gemeinsame Zuständigkeit der Aufsichtsbehörden in den betroffenen Mitgliedstaaten vor, wobei einer der Behörden die – nach objektiven Kriterien festzulegende – Federführung zukommt. Übergeordnetes Ziel ist stets der einheitliche, gleichmäßige Vollzug des Gesetzes.

Der Gesetzgeber hat auf der Grundlage der ersten Jahre an Erfahrungen mit dem gemeinsamen Vollzug der DS-GVO im Jahr 2025 mit der Verordnung zur Festlegung zusätzlicher Verfahrensregeln („DSGVO-Verfahrensverordnung“)erstmals einige Änderungen im Verfahren der Zusammenarbeit bei der Bearbeitung von Beschwerden zu grenzüberschreitenden Verarbeitungen beschlossen. Die DSGVO-Verfahrensverordnung wurde am 26.11.2025 final verabschiedet und am 12.12.2025 im Amtsblatt der Europäischen Union verkündet, die Änderungen werden jedoch erst am 2. April 2027 in Kraft treten. Erklärte Zielrichtung der Verfahrensverordnung ist es, die Bearbeitung von DS-GVO-Beschwerden bei grenzüberschreitenden Verarbeitungen zu beschleunigen, gleichzeitig aber vor dem Hintergrund des grundrechtlich

verbürgten Anspruchs auf rechtliches Gehör eine angemessene Mitwirkung aller am Verfahren Beteiligten zu wahren. Diese Ziele stehen freilich in einem gewissen Spannungsverhältnis zueinander, da die grundrechtlich gebotene Ermöglichung rechtlichen Gehörs naturgemäß bestimmte Verfahrensschritte erfordert, die mit angemessenen Fristen versehen sein müssen und damit Auswirkung auf die Verfahrensdauer haben.

Die wichtigsten Änderungen, die die Verfahrensverordnung mit sich bringt, betreffen folgende Punkte:

- Einführung einer Höchstfrist von fünfzehn Monaten für die Bearbeitung von Beschwerden zu grenzüberschreitenden Verarbeitungen (mit einer Verlängerungsmöglichkeit um max. zwölf Monate bei besonders komplexen Sachverhalten)
- Einführung der Möglichkeit eines sog. vereinfachten Verfahrens mit einer Verfahrensdauer von max. zwölf Monaten
- Harmonisierung der Kriterien für die Bewertung der Zulässigkeit von Beschwerden
- Möglichkeit einer sog. frühzeitigen Beilegung für Fälle, in denen der Verstoß beendet wurde
- weitere Harmonisierung des Verfahrens durch Einführung bestimmter zwingender Zwischenschritte im Verfahren mit definierten Vorgaben etwa zu den Informationen, die die federführende Behörde den anderen betroffenen Behörden zur Verfügung stellen muss
- frühzeitige Klarstellung des Verfahrensgegenstands
- Harmonisierung der Beteiligungsrechte für die Beschwerdeführer und die Beschwerdegegner (insbesondere Anhörungsrechte)

Gemeinsam mit den anderen deutschen und europäischen Datenschutzaufsichtsbehörden haben wir unsere praktischen Erfahrungen aus der gemeinsamen Bearbeitung von Beschwerden in mehrere Äußerungen des Europäischen Datenschutzausschusses zu diesem Gesetzesprojekt eingebracht. Ob die vom Gesetzgeber beschlossenen Änderungen und Klarstellungen in der Praxis zu einem „besseren" Verfahren führen werden, bleibt abzuwarten. Die durch die Verfahrensverordnung beabsichtigte weitere Harmonisierung des Verfahrens der Bearbeitung von Beschwerden zu grenzüberschreitenden Verarbeitungen ist auch aus unserer Sicht grundsätzlich zu begrüßen, da ein gleichmäßiger Vollzug ein wichtiges Kriterium für eine gute Akzeptanz des Gesetzes gleichermaßen bei Verfahrensbeteiligten und in der allgemeinen Öffentlichkeit ist. Gleichzeitig bleibt abzuwarten, ob die sehr ambitionierten Höchstfristen für die Bearbeitung von Beschwerden den Praxistest bestehen werden. Die praktischen Erfahrungen haben gezeigt, dass manche Beschwerdesachverhalte für die Aufsichtsbehörde einen ganz erheblichen Ermittlungsaufwand mit sich bringen, insbesondere bei Verarbeitungsprozessen mit hoher technischer Komplexität oder bei innovativen Technologien. Häufig stellen auch laufende dynamische Fortentwicklungen der untersuchten Verarbeitungen die Aufsichtsbehörden vor erhebliche Herausforderungen. Es ist daher absehbar, dass die Verfahrensverordnung vor diesem Hintergrund auch die Frage der personellen Ausstattung der Aufsichtsbehörden weiter verschärfen wird.

Zu erwarten ist in jedem Fall, dass die Regelungen der Verfahrensverordnung, die an sich nur für grenzüberschreitende Fälle zwingende Geltung beanspruchen, auch auf die Bearbeitung von Beschwerden zu rein national beschränkten

Verarbeitungssachverhalten ausstrahlen werden. Vermutlich nicht im Sinne einer 1:1-Übertragung jeder einzelnen Detailregelung, aber doch einer starken Angleichung der Verfahrensschritte bei der Bearbeitung von Beschwerden. Dies ist schon ein Erfordernis der Verfahrensökonomie, weil es für Sachbearbeiterinnen und Sachbearbeiter wesentlich einfacher sein dürfte, etwa einheitliche Muster und Fristen für grundsätzlich alle von ihnen bearbeiteten Beschwerdefälle zu verwenden. Ähnliche Überlegungen werden sicherlich auch bei anderen Aufsichtsbehörden angestellt werden. Unter den Gesichtspunkten der Verfahrenspraxis erwarten wir uns daher von der Verfahrensverordnung einen Harmonisierungsschub, der über den streng juristischen Anwendungsbereich dieser Verordnung noch deutlich hinausweisen wird.

3.3 Mitwirkung in Subgroups des EDSA

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

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

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

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

Im Berichtszeitraum stellten wir weiterhin den Landesvertreter in der International Transfer Expert Subgroup und neu gewählt, eine Landesvertreterin für die Compliance, eGovernance and Health Subgroup. Durch die Mitarbeit auf europäischer Ebene ist es uns möglich, an der Erstellung von Leitlinien, Empfehlungen und anderen Papieren des EDSA direkt mitzuarbeiten und die maßgeblichen Entscheidungen auf europäischer Ebene unmittelbar mitzugestalten.

Wir haben in den vergangenen Jahren in den Unterarbeitsgruppen für eine Reihe von Papieren (Leitlinien, interne Arbeitsanweisungen etc.) die Berichterstattung übernommen. Dies umfasst insbesondere die Erstellung von Entwürfen und die Koordinierung des Erarbeitungsprozesses sowie die Präsentation der finalen Version vor dem Plenum des EDSA.

Auch im Rahmen solcher Unterarbeitsgruppen, für die wir keine förmliche Vertretung innehatten, versuchen wir stets, uns an den Arbeiten zu beteiligen, um so auf die Positionierung der

Aufsichtsbehörden zu den von der DS-GVO aufgeworfenen Fragen auf europäischer Ebene Einfluss zu nehmen. Dies geschieht vorrangig durch eine Beteiligung an der innerdeutschen Meinungsbildung zu den angestoßenen Diskussionen und Beiträgen zu Leitlinien und anderen Entwürfen.

Im Berichtszeitraum umfasste die Subgroup-Arbeit insbesondere die Berichterstattung für das zwischenzeitlich fertiggestellte Papier „Recommendations for BCR-Processors", sowie die Arbeit an den noch nicht abgeschlossenen Guidelines des EDSA zu „Consent or pay"- Modellen.

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

4.1 Löschung der E-Mail-Adresse aus der „AutoVervollständigen-Liste“ von Microsoft Outlook

Ist die E-Mail-Adresse einer betroffenen Person gemäß Art. 17 Abs. 1 DS-GVO zu löschen, so ist diese auch aus der „AutoVervollständigen-Liste“ in Microsoft Outlook zu entfernen.

Im Berichtszeitraum erreichten uns Beschwerden von betroffenen Personen, welche rügten, dass sie durch den Beschwerdegegner per E-Mail kontaktiert worden seien, obwohl deren personenbezogenen Daten und somit auch die in den Beschwerdeverfahren verarbeiteten personenbeziehbaren E-Mail-Adresse gemäß Art. 17 Abs. 1 DS-GVO bereits hätte gelöscht sein müssen.

Im Laufe dieser Verfahren stellte sich heraus, dass die Verantwortlichen zwar (teilweise) ihrer Löschpflicht nach Art. 17 DS-GVO nachgekommen sind, allerdings dabei die E-Mail-Adresse der betroffenen Person nicht aus der „AutoVervollständigen-Liste“ in Microsoft Outlook entfernten. Durch die automatische Vervollständigung der E-Mail-Adresse im „An“, „CC“ oder „BCC“-Feld fand in der Folge ein Versand an die betroffene Person statt, da bei Versendung der E-Mail dem Versender nicht auffiel, dass eine falsche E-Mail-Adresse autovervollständigt und durch ihn ausgewählt worden war.

Ist der Verantwortliche gemäß Art. 17 Abs. 1 DS-GVO verpflichtet, die E-Mail-Adresse einer betroffenen Person zu löschen, so muss dieser Vorkehrungen schaffen, dass – soweit die „AutoVervollständigen-Liste“ genutzt wird - im Rahmen des Löschprozesses auch die E-Mail-Adresse der betroffenen Person aus der „AutoVervollständigen-Liste“ in Microsoft Outlook entfernt wird (Neue E-Mail→Adresseingabe im Anfeld→ ). Geschieht dies nicht, ist die weitere (unbewusste) Verarbeitung datenschutzrechtswidrig.

Verantwortlichen empfehlen wir deshalb, diese Datenquelle – ebenso wie z. B. E-Mail-Verteiler - in das Löschkonzept aufzunehmen, damit tatsächlich eine vollständige Löschung der personenbezogenen Daten erfolgt und es nicht doch noch zu einem (versehentlichen) Versand von E-Mails an die betroffene Person kommen kann. Alternativ kann die Einstellung „Beim Ausfüllen der Zeilen „An“, „CC“ und „BCC“ Namen mithilfe der AutoVervollständigen-Liste vorschlagen“ deaktiviert werden bzw. die „AutoVervollständigen-Liste“ geleert werden (Datei→Optionen→E-Mail→Nachricht senden→„Beim Ausfüllen der Zeilen „An“, „CC“ und „BCC“ Namen mithilfe der AutoVervollständigen-Liste vorschlagen“ bzw. „AutoVervollständigen-Liste leeren“).

Die uns vorliegenden Verfahren haben wir nach Ausübung unseres Ermessens mit der Feststellung eines Verstoßes jedoch ohne Maßnahme gem. Art. 58 Abs. 2 DS-GVO abgeschlossen.

4.2 Durchsetzung der DS-GVO in der Praxis

Datenschutzaufsichtsbehörden stellen nicht nur durch die Verhängung von Geldbußen die Einhaltung der DS-GVO sicher.

Kernaufgabe der Datenschutzaufsichtsbehörden ist es, die Einhaltung der Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu überwachen. Um diese Aufgabe erfüllen zu können, stehen den Behörden verschiedene Untersuchungs- und Abhilfemaßnahmen zur Verfügung. Die Verhängung von Geldbußen ist dabei nur eines von verschiedenen Mitteln. Wie ein

Vergleich der Fallzahlen zeigt, kommt eine solche in der Praxis - im Vergleich zu anderen Abhilfemaßnahmen - sogar nur in seltenen Fällen zur Anwendung.

Stellt die Aufsichtsbehörde einen - oder sogar mehrere - Verstöße gegen die DS-GVO fest, geht es vorrangig darum, datenschutzwidrige Verarbeitung (wieder) in Einklang mit der DS-GVO zu bringen. Die Einhaltung konkreter datenschutzrechtlicher Verpflichtungen kann gegenüber Verantwortlichen und Auftragsverarbeitern oftmals nur durch entsprechende Anweisungen und ggf. der Anwendung von Zwangsmitteln erreicht werden. Die Verhängung von Geldbußen ist hierfür kein geeignetes Mittel, da diese Verantwortlichen nur eine Zahlungspflicht, nicht jedoch eine Pflicht zur Herstellung eines datenschutzkonformen Zustandes, auferlegt. Geldbußen werden daher in der Regel nur als zusätzliche Maßnahme und auch nur bei schwerwiegenderen Verstößen festgesetzt, da die DS-GVO für geringfügige Verstöße mit der Verwarnung eine mildere Maßnahme vorsieht. Wenn ein Verstoß vorliegt und zusätzlich förmliche Anweisungen der Behörde zur (Wieder-)Herstellung eines datenschutzkonformen Zustandes missachtet werden, liegt aus unserer Sicht, unabhängig von der Art des (ursprünglichen) Verstoßes, keine Geringfügigkeit mehr vor und die Verhängung einer Geldbuße kommt neben dieser Anweisung in Betracht. Auch wenn die Festsetzung einer Geldbuße im Einzelfall unterbleibt, bedeutet dies nicht, dass die Datenschutzbehörden „zahnlose Papiertiger" sind, sondern Sie können mit Hilfe von Zwangsmitteln die entsprechenden Anweisungen durchsetzen.

Aufsichtsbehörden sind in der Regel schon bei der Ermittlung des Sachverhalts auf die Mitwirkung des Verantwortlichen angewiesen. Eine entsprechende Mitwirkungspflicht sieht Art. 31 DS-GVO vor, wonach Verantwortliche, Auftragsverarbeiter und gegebenenfalls deren Vertreter auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenarbeiten müssen. Neben dieser allgemeinen Kooperationspflicht statuiert die DS-GVO eine Reihe spezieller Zusammenarbeitspflichten, die dem Adressaten mitunter auch ein aktives Tun abverlangen, wie etwa die Pflicht, der Aufsichtsbehörde alle Informationen bereitzustellen, die sie benötigt, um ihre Aufgaben erfüllen zu können (Art. 58 Abs. 1 Buchst. a DS-GVO). Kommt der Verantwortliche seinen Pflichten nicht (freiwillig) nach, kann die Aufsichtsbehörde diesen zur Erfüllung seiner Verpflichtungen per Verwaltungsakt anweisen. Sobald eine solche förmliche Anweisung ausgesprochen wird, fallen für den Adressaten Kosten in Form von Bescheidgebühren an. Darüber hinaus kann die Durchsetzung mit Zwangsmitteln entsprechend dem Bayerischen Verwaltungszustellungs- und Vollstreckungsgesetz (BayVwZvG), wie Zwangsgeld, Ersatzvornahme oder auch Ersatzzwangshaft sichergestellt werden. Unter den Zwangsmitteln besitzt für die alltägliche Arbeit der Datenschutzaufsichtsbehörden allein das Zwangsgeld Praxisrelevanz. Durch die Androhung von Zwangsgeldern können Behörden den Pflichtigen wirksamer zur Einhaltung seiner Verpflichtungen anhalten. Kommen Adressaten ihren Pflichten nicht innerhalb der gesetzten Frist nach, ist nämlich das angedrohte Zwangsgeld zur Zahlung fällig. Das Zwangsgeld beträgt mindestens fünfzehn und höchstens fünfzigtausend Euro (Art. 31 Abs. 2 S. 1 BayVwZvG) und kann grundsätzlich solange angewandt werden, bis der Adressat seinen Verpflichtungen nachkommt.

Nicht nur bei Untersuchungshandlungen, sondern auch in anderen Fallkonstellationen, in denen Verantwortliche ihren Pflichten nicht freiwillig nachkommen, werden gebührenpflichtige Anweisungen ausgesprochen und direkt mit Fristsetzungen und Zwangsgeldandrohungen verbunden - beispielsweise im Fall nichterfüllter Betroffenenrechte oder sonstigen datenschutzwidrigen Zuständen. Wenn kostenpflichtige Anweisungen und Androhungen von Zwangsgeldern nicht ausreichen, um Verantwortliche zur Erfüllung ihrer Verpflichtungen anzuhalten,

kommt als letztes Mittel, um eine konsequente Einhaltung der DS-GVO - zumindest für die Zukunft - sicherzustellen, nur noch die Eröffnung eines Bußgeldverfahrens in Betracht. Von dieser Möglichkeit wird bei renitenten Verantwortlichen in der Praxis mittlerweile konsequent Gebrauch gemacht.

Im Berichtszeitraum hatte es das BayLDA mit einem solchen, besonders unwilligen Verantwortlichen zu tun, den Zwangsgeldandrohungen und Bescheidgebühren unbeeindruckt ließen:

Eine Bürgerin machte nach dem Kauf eines Fahrzeugs Sachmängelansprüche bei dem Verkäufer geltend. Nachdem zur Mängelbehebung plötzlich eine andere Firma mit ihr Kontakt aufnahm, machte sie bei dieser ein Auskunftsersuchen geltend, um zu erfahren, wie diese in den Besitz ihrer Daten kam. Da sie keine Reaktion auf ihr Auskunftsersuchen erhielt, legte sie bei dem BayLDA Beschwerde ein. Das Landesamt nahm Kontakt mit dem Verantwortlichen auf und gab diesem Gelegenheit, das Auskunftsersuchen der Bürgerin zu erfüllen. Bereits in dem ersten Anschreiben wurde der Verantwortliche darauf hingewiesen, dass beabsichtigt sei, diesen zur Auskunftserteilung anzuweisen, wenn das Auskunftsersuchen nicht erfüllt werde. Nachdem keine Reaktion des Verantwortlichen erfolgte, nahm das BayLDA telefonisch Kontakt mit diesem auf und verwies auf die Dringlichkeit. Obwohl dem Verantwortlichen das Schreiben mit weiteren Informationen zum Auskunftsrecht anschließend erneut per E-Mail übersandt wurde, erfolgte weiterhin keine Reaktion, so dass das Landesamt den Verantwortlichen mit kostenpflichtigem Bescheid zur Auskunftserteilung, Bestätigung der Erledigung und Darlegung der Gründe für die nicht fristgerechte Beantwortung, hilfsweise der Verweigerungsgründe, anwies. Für den Fall, dass der Verantwortliche diesen Pflichten nicht innerhalb der gesetzten Fristen nachkam, wurden Zwangsgelder in einer Höhe von 5.000 Euro (Auskunftserteilung) und 2.500 Euro (schriftliche Bestätigung der Erledigung und Darlegung der Gründe für die nicht fristgerechte Auskunftserteilung) angedroht. Der Bescheid wurde bestandskräftig, ohne dass der Verantwortliche seine Pflichten erfüllte. Das Bayerische Landesamt für Datenschutzaufsicht informierte den Verantwortlichen über die Fälligkeit der Zwangsgelder und forderte diesen zur Zahlung auf. Gleichzeitig wurden neue Fristen gesetzt und erneut Zwangsgelder - wieder in einer Höhe von 5.000 Euro und 2.500 Euro – angedroht.

Dies veranlasste den Verantwortlichen jedoch – ebenso wenig wie weitere, folgende und in der Höhe ansteigende Zwangsgeldandrohungen – zur Erfüllung seiner Verpflichtungen. Aufgrund der beharrlichen Weigerung des Verantwortlichen, seinen Pflichten nachzukommen, wurde der Vorgang von dem Fachbereich an die Zentrale Bußgeldstelle abgegeben. Auch hier reagierte der Verantwortliche auf die Anhörung nicht, beglich jedoch zwischenzeitlich fällig gewordene Bescheidgebühren, Zwangsgelder und Mahngebühren in einer Gesamthöhe von über 15.000 Euro. Nachdem darüber hinaus keine Reaktion des Verantwortlichen erfolgte, dieser insbesondere den Anweisungen weiterhin nicht nachkam, wurden schließlich zwei Geldbußen in einer Gesamthöhe von 50.000 Euro festgesetzt. Ob der Verantwortlichen auch diesen Bescheid akzeptieren wird und ihn die verhängten Geldbußen in Zukunft zu einem datenschutzkonformen Verhalten veranlassen werden, bleibt abzuwarten. Insgesamt wurden, in diesem Verfahren, bis Redaktionsschluss fünf Mal Zwangsgelder mit einer Gesamtsumme von 66.000 Euro angedroht, was gemeinsam mit den festgesetzten Geldbußen bereits jetzt zu einer Zahlungspflicht von über 100.000 Euro führen würde, wenn der Verantwortliche seinen Pflichten weiterhin nicht nachkommt.

5

Datenschutzbeauftragte

5 Datenschutzbeauftragte

5.1 Bereitstellung einer separaten Kontaktmöglichkeit zu Datenschutzbeauftragten (DSB)

Zur Wahrung der Vertraulichkeit, ist von Verantwortlichen ein separater Kontaktkanal zum DSB bereitzustellen.

In regelmäßigen Abständen werden wir darauf aufmerksam, dass Verantwortliche, die entweder aufgrund bestehender Verpflichtung oder freiwillig einen DSB benannt haben, in ihren Datenschutzinformationen nach Art. 13 / 14 DS-GVO für den Kontakt zum Verantwortlichen und für den Kontakt zum DSB jeweils eine identische E-Mail-Adresse angeben. Dies bewerten wir als unzulässig.

DSB sind bei der Erfüllung ihrer Aufgaben an die Wahrung der Geheimhaltung / Vertraulichkeit gebunden (Art. 38 Abs. 5 DS-GVO), was nicht gewährleistet werden kann, wenn eine betroffene Person, die einen DSB zu Rate ziehen möchte, hierfür eine Kontaktmöglichkeit nutzen muss, die auch vom Verantwortlichen eingesehen wird.

Entsprechend Art. 38 Abs. 2 DS-GVO hat der Verantwortliche dafür Sorge zu tragen, dass der DSB über ausreichende Ressourcen zur Erfüllung seiner Aufgaben verfügt. Hierzu gehört es also auch, zu diesem eine separate Kontaktmöglichkeit bereitzustellen, zu welcher nur der jeweilige DSB und ggf. eine benannte Stellvertretung oder dem DSB weisungsmäßig unterstelltes Personal Zugang haben.

Bzgl. eines E-Mail-Kontakts kann dies regelmäßig durch eine entsprechend eingerichtete Funktionsadresse, wie z. B. „dsb@...“ umgesetzt werden.

Analog hat der Verantwortliche auch zu gewährleisten, dass postalische Eingänge, die dem DSB z. B. durch einen Adresszusatz „Datenschutzbeauftragter“ eindeutig zuzuordnen sind, direkt und ungeöffnet an den DSB zugeleitet werden.

6

Finanzwirtschaft

6 Finanzwirtschaft

6.1 Beschwerden zu Forderungsstreitigkeiten

Die Datenschutzaufsicht kann nicht über den rechtlichen Bestand zivilrechtlicher Forderungen entscheiden.

Im Berichtszeitraum haben wir eine deutliche Zunahme von Eingaben festgestellt, die im Wesentlichen zum Thema hatten, dass gegenüber der betroffenen Person eine Geldforderung geltend gemacht wird; entweder direkt durch die mutmaßlichen Gläubigerinnen und Gläubiger oder auch durch ein Inkassounternehmen.

Uns wird in diesem Zusammenhang dann von den betroffenen Personen z. B. dargestellt, dass sie mit den Beteiligten keinen Kontakt hatten, keinen Vertrag geschlossen haben, einen geschlossenen Vertrag fristgerecht widerrufen haben oder die Forderung aus anderen Gründen dem Grunde nach oder ihrer Höhe nach ungerechtfertigt sei. Anhand dieser Darstellung gehen die betroffenen Personen davon aus, dass die Verarbeitung ihrer personenbezogenen Daten bei den Stellen, die die Forderung geltend machen, unzulässig ist und diese zur Löschung ihrer Daten verpflichtet wären.

Wir können in diesen Fällen als Datenschutzaufsicht aber regelmäßig nicht weiterhelfen, da die Kernfrage in solchen Fällen ist, ob die Geldforderung zivilrechtlich tatsächlich Bestand hat oder nicht. Die zivilrechtliche Beurteilung kann im Streitfall ausschließlich über die Zivilgerichte erfolgen. Wir können und dürfen hierzu nicht entscheiden.

Diese zivilrechtliche Klärung kann auch nicht datenschutzrechtlich, z. B. durch einen Widerspruch oder durch ein Löschersuchen, sozusagen „umgangen“ werden. So ist ein Widerspruchsrecht nach Art. 21 Abs. 1 DS-GVO, welches zudem hohen Anforderungen hinsichtlich "besonderer Gründe" unterläge, bei Verarbeitungen die der Geltendmachung von Rechtsansprüchen dienen, generell ausgeschlossen. Bzgl. einer Löschung dürfte es im Stadium der strittigen Forderung bereits an einer hinreichend geklärten Löschpflicht nach Art. 17 Abs. 1 DS-GVO fehlen. Spätestens die Löschausnahme aus Art. 17 Abs. 3 Buchst. e DS-GVO würde eine Löschung in dieser Situation jedoch verhindern.

Entgegen einer verbreiteten Fehlannahme ist es Inkassounternehmen zudem auch nicht verboten, in der Beitreibung strittiger Forderungen tätig zu werden.

Wir können also in solchen Situationen in der Regel nur empfehlen, zunächst den zivilrechtlichen Bestand der Forderung zu klären. Datenschutzrechtlich kann es zudem in der geschilderten Situation empfehlenswert sein, gegenüber den Verfahrensbeteiligten den Bestand der Forderung substantiiert zu bestreiten, da dies unter Umständen bis zur weiteren Klärung der Forderungsstreitigkeit die Vornahme von Negativmeldungen an Wirtschaftsauskunfteien hindern kann.

Sofern unklar ist, woher die Stelle, die die Forderung geltend macht, die Daten der betroffenen Person bezogen hat, oder generell Fragen dahingehend bestehen, welche Daten der betroffenen Person verarbeitet werden, kann beim entsprechenden Unternehmen / Inkasso ein Auskunftsersuchen nach Art. 15 DS-GVO geltend gemacht werden.

Bei Annahme eines Betrugsfalls oder einer sonstigen Straftat, wären zusätzlich die Strafverfolgungsbehörden geeignete Ansprechpartner.

6.2 Bonitätsabfragen durch Inkassodienstleister vor erster Kontaktaufnahme

Bonitätsabfragen durch Inkassodienstleister, die bereits vor ihrem ersten Kontakt mit Schuldnerinnen und Schuldnern erfolgen, sind in der Regel unzulässig.

Wir hatten einen Vorgang zu beurteilen, bei welchem ein Inkassodienstleister direkt nach Übernahme des Auftrags eine Bonitätsabfrage zur betroffenen Person bei einer Wirtschaftsauskunftei vorgenommen hat, ohne dass er mit dieser zuvor den Kontakt zur Forderungssache gesucht hatte.

Die Zulässigkeit einer solchen Bonitätsabfrage ist anhand von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zu beurteilen. Der Inkassodienstleister muss also eine Interessensabwägung vornehmen.

Ein Automatismus, eine Bonitätsabfrage bereits unmittelbar nach Übernahme des Inkassoauftrags vorzunehmen, ist datenschutzrechtlich regelmäßig unzulässig, da zu diesem Zeitpunkt ein hinreichendes berechtigtes Interesse nicht anzunehmen ist.

In der Regel besteht ein solches hinreichendes berechtigtes Interesse dann, wenn die Erfolgsaussichten kostenintensiver Beitreibungsmaßnahmen geprüft werden, wie z. B. die Beantragung eines Mahnbescheids; frühestens jedenfalls zu einem Zeitpunkt, zu dem die betroffene Person vom Inkassodienstleister ein Schreiben zur Zahlungsaufforderung erhalten und Gelegenheit zur Stellungnahme hatte.

Ausnahmen hiervon können im Einzelfall denkbar sein, z. B. wenn der Inkassodienstleister ausgemahnte, bereits titulierte Forderungen zur Beitreibung übernimmt, bzgl. derer die vorherigen Beitreibungsbemühungen fruchtlos waren.

Die Situation einer Inkassodienstleistung, bei der das Inkassounternehmen im Auftrag zur Beitreibung tätig wird, muss zudem von der Situation unterschieden werden, in welcher das Inkassounternehmen die Forderung im Rahmen eines Forderungskaufs übernimmt, also durch Übertragung der Rechte zum neuen Forderungsinhaber wird. In dieser Situation kann eine Bonitätsabfrage bereits vor dem Ankauf der Forderung zulässig sein.

6.3 Unzureichende Löschprozesse nach dem Zusammenschluss zweier Kreditinstitute

Gesellschaftliche Veränderung entbinden einen Verantwortlichen nicht von der zeitgerechten Erfüllung datenschutzrechtlicher Verpflichtungen.

Im Rahmen der Prüfung einer Beschwerde, stellten wir fest, dass ein Kreditinstitut geraume Zeit nach Ablauf gesetzlicher Aufbewahrungspflichten oder sonstiger Aufbewahrungserfordernisse noch über Daten der betroffenen Personen, z. B. zu beendeten Verträgen, verfügte.

Begründet wurde dies vom Kreditinstitut im Wesentlichen damit, dass es sich um Daten handle, die das Kreditinstitut im Rahmen eines früheren Zusammenschlusses mit einem anderen Kreditinstitut erhalten habe. Aufgrund der langwierigen technischen Integration, manuellen Prüferfordernissen und anderen regulatorisch parallel erforderlichen technischen Umstrukturierungen, sei es bislang noch nicht gelungen, die Daten des zweiten Kreditinstituts vollständig in die eigenen Löschprozesse zu integrieren.

Im Rahmen unserer Prüfung stellten wir allerdings fest, dass dies unter anderem aufgrund der Tatsache, dass der gesellschaftsrechtliche Zusammenschluss bereits mehrere Jahre zurücklag, durchaus möglich gewesen wäre.

Im Ergebnis hat das Kreditinstitut damit nicht nur gegen seine Löschpflichten verstoßen, sondern hatte damit zusammenhängend auch keine datenschutzrechtliche Zulässigkeitsgrundlage für die weitere Verarbeitung der eigentlich löschpflichtigen Daten mehr. Das Kreditinstitut hat seinen Datenbestand im Verlauf unseres aufsichtlichen Verfahrens entsprechend bereinigt.

7

Werbung

7 Werbung

7.1 Anforderungen an den Nachweis einer wirksamen Einwilligung für Direktwerbung

Anforderungen an den Nachweis einer wirksamen Einwilligung für Direktwerbung.

Während des Berichtzeitraums konnte im Werbebereich ein Anstieg von Beschwerdefällen beobachtet werden, welchen der folgende Sachverhalt zugrunde liegt:

Die betroffenen Personen erhalten personalisierte Werbe-E-Mails, Newsletter oder Werbeschreiben von verantwortlichen Stellen, die den betroffenen Personen gänzlich unbekannt sind. Auf Nachfrage zur Herkunft der personenbezogenen Daten (vgl. Art. 15 Abs. 1 Buchst. g DS-GVO) und auf welcher Rechtsgrundlage diese verarbeitet werden, wurde in einigen uns vorliegenden Fällen angegeben, die betroffenen Personen hätten an einem Online-Gewinnspiel teilgenommen. Im Rahmen des Registrierungsprozesses zum Gewinnspiel sei die Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO zur Verarbeitung der personenbezogenen Daten zum Zwecke der werblichen Ansprache erteilt worden. Diese würde mittels des sog. Double-Opt-In-Verfahrens eingeholt, bei welchem der Einwilligende durch das Anklicken eines zugesendeten Links seine Einwilligung erteilt.

Die betroffenen Personen bestreiten oft die Teilnahme an den Gewinnspielen, jedenfalls aber die Erteilung einer entsprechenden Einwilligung im Rahmen des Registrierungsprozesses. In einem Fall konnte auch glaubhaft dargelegt werden, dass sich die betroffene Person zum angegebenen Zeitpunkt der Bestätigung außer Landes aufgehalten hat und weder sie noch jemand anderes die angebliche Einwilligung unter der angegebenen IP-Adresse erteilen konnte.

Die Online-Gewinnspiele wurden meist von Dritten veranstaltet, deren Sitz im EU-Ausland liegt. Die Gewinnspiele wurden von sogenannten Sponsoren unterstützt bzw. beauftragt, die dann oftmals als Werbetreibende, mithin die in den Beschwerden benannten Beschwerdegegner, in Erscheinung treten. Der Datenübermittlung vom Gewinnspielbetreiber zum Werbetreibenden sind zudem teilweise vermittelnde Unternehmen zwischengeschaltet, deren Geschäftsmodell die Kundenakquise ist. Auch gegen diese richten sich Beschwerden.

Sowohl die Werbetreibenden als auch die Datenvermittler stützen die Verarbeitung der personenbezogenen Daten der betroffenen Personen auf die von den Gewinnspielbetreibern (vermeintlich) – auch für die Bewerbung durch Sponsoren - eingeholte Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO.

Als Nachweis der wirksam erteilten Einwilligung werden in tabellarischer Form das (vermeintliche) Datum des Double-Opt-In, die IP-Adresse der betroffenen Person samt Zeitstempel, der entsprechende URL-Link des Gewinnspiels sowie die Sponsoren angegeben.

Diese Angaben genügen nach unserer Auffassung, sowie der Rechtsprechung des Bundesgerichtshofs den Anforderungen an einen Nachweis der wirksam und informiert erteilten Einwilligung nicht.

Die Nachweispflicht obliegt gemäß Art. 7 Abs. 1 DS-GVO dem Verantwortlichen. Verantwortlicher ist jede Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 4 Nr. 7 DS-GVO. Die Pflicht zum Nachweis einer wirksamen Einwilligung obliegt damit sowohl dem Gewinnspielbetreiber, als auch den die Daten vermittelnden Akteuren und Werbetreibenden, welche die Daten verarbeiten

und sich hierbei auf die erteilte Einwilligung stützen.

Nach Art. 4 Nr. 11 DS-GVO ist eine Einwilligung der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

In seiner Entscheidung vom 10.02.2011, Az. I ZR 164/09, führt der Bundesgerichtshof konkretisierend aus, dass eine Einwilligung vollständig nachweisbar sein muss, auch hinsichtlich ihres Wortlautes. Der Verantwortliche hat die konkrete Einverständniserklärung jeder einzelnen betroffenen Person vollständig zu dokumentieren. Im Fall einer elektronisch übermittelten Einverständniserklärung setzt das deren Speicherung und die jederzeitige Möglichkeit voraus, sie auszudrucken. Das bloße Abspeichern einer IP-Adresse und die Behauptung, dass von dieser eine Einwilligung erteilt worden sei, genügen den Anforderungen an eine Nachweisbarkeit nicht. In der genannten Entscheidung des Bundesgerichtshofes wird die Vorlage einer Bestätigungs-E-Mail als Nachweismöglichkeit angesprochen; bei einer solchen könnte anhand der eingesetzten digitalen Signaturen (z. B. DKIM-Signatur) die Authentizität der E-Mails und damit der Einwilligung nachgewiesen werden. Entsprechende Ausführungen finden sich auch in der Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung https://www.datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf, Abschnitt 3.3.)

Allerdings obliegt es dem Verantwortlichen zu entscheiden, auf welche Weise ein entsprechender Nachweis für das Vorliegen einer wirksamen Einwilligung der betroffenen Person erbracht wird. Hierzu auch der Europäische Datenschutzausschuss, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1., Kapitel 5.1 edpb_guidelines_202005_consent_de.pdf.

Wir empfehlen den Verantwortlichen daher, bereits im Vorfeld eine möglichst beweis- und fälschungssichere Möglichkeit der Dokumentation von Einwilligungserklärungen sicherzustellen. Insbesondere dann, wenn wir eine Häufung von entsprechenden Beschwerden bei Verantwortlichen feststellen, verlangen wir einen entsprechenden Nachweis.

8

Industrie und Handel, Wohnungswirtschaft

8 Industrie und Handel, Wohnungswirtschaft

8.1 Personalausweise – Kopie und Pfand mit hohem Missbrauchsrisiko

Die Anfertigung und das Anfordern von Personalausweiskopien entbehren regelmäßig einer datenschutzrechtlichen Befugnis und bergen ein hohes Risiko.

Im Berichtszeitraum erreichte uns weiterhin eine hohe Anzahl an Beschwerden, die die Verarbeitung der auf dem Personalausweis enthaltenen personenbezogenen Daten betrafen. Insbesondere ging es um die Anfertigung von Kopien der Ausweise und Anforderung von Scans durch die Ausweisinhaberin bzw. den Ausweisinhaber im Bereich Beherbergung.

Die Frage nach einer Personalausweiskopie

Zwar haben wir bereits in unserem 8. Tätigkeitsbericht 2017/2018, Kapitel 13 darauf hingewiesen, dass zur Feststellung der Identität im Regelfall eine Sichtprüfung genügt, allerdings werden Personalausweiskopien weiterhin scheinbar reflexartig, aus Unsicherheit oder in dem Glauben, dass auch Personalausweiskopien belastbare Dokumente zur Identifizierung von Personen sind, in zahlreichen Konstellationen ungeachtet der Eignung, der Erforderlichkeit und der Missbrauchsrisiken gefordert und angefertigt.

Die breite Akzeptanz von Personalausweiskopien durch Verantwortliche zu Nachweiszwecken und auch die Sorglosigkeit einiger betroffener Personen ist vor dem Hintergrund der hohen Missbrauchsrisiken sehr bedenklich. Immer wieder (so auch in diesem Jahr) wird in der Presse über Personalausweiskopien berichtet, die nach Hacking-Angriffen im Darknet auftauchen.

Nicht umsonst enthält der Personalausweis viele einzigartige Sicherheitsmerkmale, so dass Missbrauch, Verfälschung oder Totalfälschung zuverlässig erkannt werden können. Ein solches Erkennen ist bei Kopien oder Scans, die ohne weiteres vervielfältig werden können, nicht möglich. Personalausweiskopien werden z. B. durch Betrüger nach einem Hacking-Angriff durch die Täter oder weitere Personen unter anderem dazu genutzt, um unter falscher Identität einen Online-Betrug zu begehen, weitere Informationen auszuspähen oder auch Bankkonten im Ausland zu eröffnen.

Ungeachtet dessen, dass in Fällen, in denen eine andere Person eine Ausweiskopie anfertigt oftmals die Zustimmung des Ausweisinhabers fehlt und insbesondere dann, wenn der Ausweis eingescannt wird, die Ablichtung nicht eindeutig als Kopie gekennzeichnet wird, ist die Anfertigung und das Verlangen nach einer (ungeschwärzten) Personalausweiskopie grundsätzlich unzulässig. Eine datenschutzrechtliche Befugnis liegt selten vor, da im Regelfall bereits die Erforderlichkeit nicht bejaht werden kann.

Personalausweiskopien im Bereich Beherbergung

Im Berichtszeitraum erreichten uns auch häufig Beschwerden aus dem Bereich der sog. Self-Check-In Unterkünfte. Dabei handelt es sich um Unterkünfte ohne klassische Rezeption / Check-In, von deren Leiterinnen und Leitern vor der Anreise ein Ausweisscan des Gastes angefordert wurde.

Als Verarbeitungszwecke wurden uns in den entsprechenden Fällen die Identitätsbestätigung des Gastes, die Vermeidung der Vermietung an Gäste, die unter falscher Identität einchecken sowie die Sicherung von Ansprüchen für den Fall etwaiger Schäden, genannt. Solche Verarbeitungen halten wir für ungeeignet, da die Tatsache, dass dem Verantwortlichen eine

Kopie eines Personalausweises zugeschickt wurde, nicht zwingend bedeutet, dass der Kommunikationspartner auch tatsächlich Inhaber des Personalausweises ist. Vielmehr könnte der Verantwortliche lediglich die Vermutung anstellen, dass es sich tatsächlich um die Person, die in dem Ausweisdokument benannt ist, handelt. Dasselbe gilt für die (zusätzliche) Anforderung eines Selfies des Ausweisinhabers. Zudem genügt die Besorgnis, dass während der Dauer der Anmietung Schäden verursacht werden, die von dem Gast zu vertreten sind, nicht dem datenschutzrechtlichen Erforderlichkeitsgrundsatz.

Einige „klassische" Beherbergungsbetriebe trugen uns außerdem vor, dass die Anfertigung einer Personalausweiskopie beim Check-In im Zusammenhang mit der Meldebescheinigung erforderlich sei. Ein Erfordernis, Personalausweiskopien anzufertigen ergibt sich auch aus den bis zum Ende des Jahres 2024 bestehenden Regelungen im Bundesmeldegesetz (BMG) jedoch nicht. Vielmehr verlangte § 29 BMG a.F., dass Personen aus dem Inland einen Meldeschein unterschreiben müssen. U. a. musste der Meldeschein die Seriennummer des Ausweisdokuments enthalten. Eine Verpflichtung zur Anfertigung einer Kopie des Personalausweises und damit eine entsprechende Verarbeitungsbefugnis bestand jedoch auch nach der bis zum 31.12.2024 geltenden Rechtslage nicht. Seit der Gesetzesänderung zum 01.01.2025 besteht die Pflicht zum Vorhalten und Unterschreiben von Meldebescheinigungen nur noch im Hinblick auf ausländische Personen. Nur insoweit musste und muss der Leiter bzw. die Leiterin der Beherbergungsstätte auch nach der aktuellen Rechtslage die Angaben im Meldeschein mit dem Identitätsdokument abgleichen; eine Kopie des Ausweisdokuments ist auch hier nicht erforderlich.

Personalausweis als Pfand

Häufig erreichten uns zuletzt außerdem Beschwerden, die sich darauf bezogen, dass Personalausweise als Pfand verlangt wurden. Beispielsweise konnte auf einem Festival eine Akkubox zur unabhängigen Stromversorgung mitsamt Power-Flatrate ausgeliehen werden, wenn hierfür ein Personalausweis als Pfand hinterlegt wurde. In einem anderen Fall wurden Personalausweise von Vater und Sohn einbehalten, um sicherzustellen, dass der noch nicht volljährige Sohn die Veranstaltung um 24:00 Uhr verlässt.

§ 1 Abs. 1 Satz 3 des Personalausweisgesetzes verbietet es, vom Personalausweisinhaber zu verlangen, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben. Hintergrund ist, dass die Hinterlegung des Personalausweises einen Missbrauch begünstigen könnte. Laut Gesetzesbegründung sollte auch eine freiwillige Abgabe nicht erfolgen (vgl. BT-Drs. 16/10489, 32).

In beiden Fällen wiesen wir die Verantwortlichen gem. Art. 58 Abs. 1 Buchst. d DS-GVO auf die Rechtslage und darauf hin, dass eine Befugnis zur Einbehaltung des Personalausweises als Pfand nicht zulässig war.

Verantwortliche sollten aus diesem Grund intensiv prüfen, ob und inwieweit eine Befugnis für das Anfordern sowie die Anfertigung von Personalausweiskopien überhaupt besteht, welche personenbezogenen Daten erforderlich sind und Schwärzungen sie anbieten bzw. selbst vornehmen müssen und welche angemessenen technische und organisatorische Maßnahmen zu ergreifen sind.

Gleichermaßen sind betroffene Personen gut beraten, dann, wenn eine Personalausweiskopie verlangt wird, zu hinterfragen, ob und inwieweit dies zulässig ist.

Ausblick

Auf Vorschlag des BayLDA wurde in der Zuständigkeit des Arbeitskreises Wirtschaft der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder ein Unterarbeitskreis eingerichtet, der sich in Federführung des BayLDA bereits in mehreren Sitzungen intensiv mit dem Thema Personalausweiskopien in datenschutzrechtlicher Hinsicht befasst hat. Die Abstimmungen sind in den finalen Zügen. Über die Ergebnisse werden wir anschließend berichten.

8.2 Auch Privatpersonen können zum Verantwortlichen werden

Auch Privatpersonen innerhalb einer Wohnungseigentümergemeinschaft (WEG) können datenschutzrechtlich Verantwortliche werden.

Im Berichtszeitraum bearbeiteten wir eine Beschwerde, in der geschildert wurde, dass mehrere Bewohnerinnen und Bewohner einer Liegenschaft aufgefordert wurden, Verstöße einer namentlich mit Anschrift und Wohnung genannten Familie gegen die Hausordnung an eine eigens hierfür eingerichtete E-Mail-Adresse zu melden. Die Aufforderung wurde von einer der Hausverwaltung zugehörigen E-Mailadresse verschickt, jedoch im Namen einer Privatperson verfasst.

In der von uns angeforderten Stellungnahme wurde sich darauf berufen, dass die Person die E-Mail-Adresse auf Anregung der Hausverwaltung eingerichtet habe, um etwaige Verstöße zu dokumentieren und zu bündeln. Der Aufruf wurde per E-Mail an über 300 Empfänger verschickt.

Die Datenschutz-Grundverordnung haben wir in dem vorliegenden Fall für anwendbar gehalten und die Privatperson, in deren Namen die E-Mail verfasst wurde, im datenschutzrechtlichen Sinne als Verantwortlichen gesehen.

Die Frage der Anwendbarkeit der DS-GVO bestimmt sich nicht danach, ob die Datenverarbeitung im Rahmen einer kommerziellen Tätigkeit erfolgt. Danach gilt die DS-GVO grundsätzlich auch für Privatpersonen. Ausgenommen sind mit der sog. Haushaltsausnahme lediglich Verarbeitungen durch natürliche Personen, die zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten erfolgen (Art. 2 Abs. 2 Buchst. c DS-GVO). Nach Erwägungsgrund 18 wird als Abgrenzungskriterium das Fehlen jeglichen Bezugs zu einer beruflichen oder wirtschaftlichen Tätigkeit in Bezug auf die vorgenommene Datenverarbeitung genannt.

Zentrales Kriterium für die Anwendbarkeit der sog. Haushaltsausnahme – und damit Nichtanwendbarkeit der DS-GVO - ist die Zurechenbarkeit der Datenverarbeitung zum privaten Bereich. Hierbei ist zu beachten, dass sich die Ausdrücke persönlich und familiär auf die Tätigkeit der Person, die personenbezogene Daten verarbeitet, und nicht auf die Person, deren Daten verarbeitet werden, bezieht (vgl. EuGH. Urteil v. 10.07.2018 – C-25/17). Die rein persönliche bzw. familiäre Sphäre war im vorliegenden Fall jedoch deutlich verlassen und die DS-GVO damit anwendbar.

Die Privatperson (und nicht die Hausverwaltung) war im vorliegenden Fall auch als Verantwortlicher i. S. d. Art. 4 Nr. 7 DS-GVO einzuordnen. Denn mit der an die Empfänger gerichteten Aufforderung, Verstöße gegen die Hausordnung an die dafür vorgesehene E-Mail-Adresse zu melden, um diese gesichtet und gebündelt an die Hausverwaltung vorzulegen, entschied die Privatperson über die Zwecke und mit der Einrichtung der entsprechenden E-Mail-Adresse auch über die Mittel der Verarbeitung.

Aus der Anwendbarkeit der DS-GVO resultieren für einen Verantwortlichen bestimmte datenschutzrechtliche Pflichten, die einzuhalten und

gegenüber der Aufsichtsbehörde ggf. nachzuweisen sind (Art. 5 Abs. 2 DS-GVO). Dies betrifft insbesondere das Erfordernis des Bestehens einer Rechtsgrundlage (Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 DS-GVO), die Einhaltung der Informationspflichten (Art. 12 ff. DS-GVO) und das Treffen geeigneter technisch-organisatorischer Maßnahmen (Art. 32 DS-GVO). Da der Verantwortliche die Verarbeitungen nach unserem Einschreiten umgehend einstellte, das Postfach löschte und sich einsichtig zeigte, konnten wir den Fall mit einer ausführlichen Belehrung abschließen.

8.3 Rauchwarnmelder mit Raum- und Klimamonitoring

Rauchwarnmeldern mit aktiviertem Raum- und Klimamonitoring dürfen nur mit einer rechtswirksamen Einwilligung eingesetzt werden.

Nach den bauordnungsrechtlichen Vorgaben müssen Wohnungen in Bayern spätestens seit dem 01.01.2018 mit Rauchmeldern ausgestattet sein (Art. 46 Abs. 4 Satz 3 der Bayerischen Bauordnung). Da die Geräte in der Regel über einen zehnjährigen Zeitraum betrieben werden können, steht in einigen Fällen zeitnah der Austausch der Rauchmelder an. Wie auch in anderen Lebensbereichen, hat die Technologie hier in der Zwischenzeit einen Schritt nach vorne gemacht und bietet smarte Lösungen an. Neuere Generationen von Rauchwarnmeldern ermöglichen insofern – neben der Erkennung und Meldung von Bränden – auch ein sogenanntes Raum- und Klimamonitoring. Die Ergebnisse werden lokal gespeichert und können je nach Gerät zudem in aufbereiteter Form über eine App eingesehen werden. Diese Zusatzfunktionen können die Vermeidung von Substanz- und Gesundheitsschäden durch Schimmelschäden infolge fehlerhaften Lüftungsverhaltens und die Senkung der Heizkosten bzw. des CO2 Ausstoßes durch gezielteres Lüften ermöglichen.

Das Raum- und Klimamonitoring ist datenschutzrechtlich jedoch relevant, da sich aus den erhobenen Daten Erkenntnisse über das Verhalten der Wohnungsbewohnerinnen und -bewohner ableiten lassen und somit eine Verarbeitung personenbezogener Daten vorliegt. So lässt sich beispielsweise aus dem Anstieg der Luftfeuchtigkeit in der jeweiligen Wohnung ableiten, dass die Bewohnerinnen bzw. Bewohner Kochen, Duschen bzw. Baden oder sich mehr Personen als üblich in der Wohnung aufhalten. In diesem Zusammenhang erhielten wir im Berichtszeitraum mehrere Anfragen.

Damit bedarf es für eine rechtskonforme Verarbeitung und ggf. Speicherung der Daten aus dem Raum- und Klimamonitoring einer tauglichen Rechtsgrundlage. Aus unserer Sicht ist die Verarbeitung in diesem Zusammenhang rechtlich nur möglich, wenn die betroffene(n) Person(en) ihre Einwilligung erteilt haben. Eine Verarbeitung auf Grundlage des berechtigten Interesses ist im Regelfall nicht möglich, da die private Wohnung als Kernbereich der privaten Lebensführung betroffen ist, welche grundgesetzlich besonderen Schutz genießt.

Datenschutzrechtlich müssen Verantwortliche also vor der Inbetriebnahme der (Zusatz-)Funktion eines Rauchmelders mit Raum- und Klimamonitoring die Einwilligung der betroffenen Person(en) einholen, die in freiwilliger und informierter Weise erfolgen muss. Andernfalls muss das Gerät mit deaktiviertem Raum- und Klimamonitoring installiert werden. Entsprechendes gilt selbstverständlich auch im Falle eines Mieterwechsels.

Insoweit ist auch darauf hinzuweisen, dass es den Anforderungen an die freiwillige Erteilung einer Einwilligung regelmäßig nicht genügen wird, wenn bspw. der Abschluss eines Mietvertrages an die Erteilung einer Einwilligung geknüpft wird oder dessen Fortbestehen davon abhängig gemacht wird. Selbstverständlich müssen Verantwortliche dabei auch mit dem Widerruf von Einwilligungen umgehen können

und die (Zusatz-)Funktionen in diesem Fall umgehend deaktivieren.

Eigentümerinnen und Eigentümern ist daher zu raten, vor dem Einbau sorgfältig zu prüfen, welche Funktionen die neuen Geräte besitzen und zusätzliche Funktionen des Raum- und Klimamonitorings zu deaktivieren, wenn eine Einwilligung der betroffenen Person(en) nicht oder noch nicht vorliegt.

9

Beschäftigtendatenschutz

9 Beschäftigtendatenschutz

9.1 Veröffentlichung personenbezogener Daten des Geschäftsführers im Handelsregister

Auch bei der Einreichung von Dokumenten beim Registergericht zum Eintrag in das Handelsregister sind die Grundsätze der Rechtmäßigkeit und der Datenminimierung zu beachten. Dies gilt auch dann, wenn die Antragstellung durch einen Notar erfolgt.

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

Uns erreichte eine Beschwerde eines ehemaligen Geschäftsführers, welcher uns mitteilte, dass der Umstand seiner Kündigung durch seine ehemalige Arbeitgeberin an das Registergericht weitergegeben worden sei und im Handelsregister veröffentlicht wurde.

Tatsächlich wurde ein Gesellschafterbeschluss im Handelsregister veröffentlicht, mit welchem zum einen die Abberufung des Geschäftsführers, aber eben auch die Anweisung des verbleibenden Geschäftsführers zur Kündigung des Beschwerdeführers beschlossen wurde.

Eine Rechtsgrundlage zum Austausch der Dokumente durch das Registergericht, d. h. in dem konkreten Fall die Ersetzung des veröffentlichten Beschlusses durch z. B. den geschwärzten Beschluss war im vorliegenden Fall nicht ersichtlich. Das Registergericht verweigerte zudem die Löschung im Sinne einer Entfernung aus dem Handelsregister gegenüber dem Beschwerdeführer.

Hinsichtlich der im Handelsregister hinterlegten Informationen gelten die Grundsätze der Registerwahrheit und der Registerkontinuität. Zwar sieht § 9 Abs. 7 HRV ein Verfahren zum Austausch von Dokumenten im Handelsregister vor. § 9 Abs. 7 HRV stellt dabei allerdings keine eigenständige Anspruchsgrundlage für einen Austausch dar, sondern regelt lediglich die Durchführung eines solchen Dokumentenaustauschs, vgl. OLG München, Beschluss vom 25.04.2024, Az. 34 Wx 90/24e.

Art. 17 Abs. 1 DS-GVO findet gemäß Abs. 3 Buchst. b im Registerwesen aufgrund der fortlaufenden Transparenz- und Beweisfunktion keine Anwendung. Eine Entfernung von vorhandenen Eintragungen durch technische Eingriffe oder sonstige Maßnahmen ist dem Registergericht nach § 387 II FamFG, § 12 S. 2 HRV untersagt. Die Löschung einer unzulässigen Eintragung erfolgt gemäß § 395 Abs. 1 S. 2 FamFG, §§ 16, 19 HRV nicht etwa durch Entfernung der Eintragung im Handelsregister, sondern stattdessen durch Eintragung eines Vermerks über die Löschung.

Die Einstellung von Dokumenten in das Handelsregister, welche überobligatorische personenbezogene Daten enthalten, kann damit – wie im vorliegenden Fall - einen irreversiblen Eingriff in das Persönlichkeitsrecht der betroffenen Personen darstellen.

Durch die Weitergabe des Gesellschafterbeschlusses, welcher auch den Auftrag zur Kündigung des Beschwerdeführers enthielt, an den Notar zur Anmeldung der Eintragung in das Handelsregister, verstieß die Arbeitgeberin insbesondere gegen den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a DS-GVO i. V. m Art. 6 Abs. 1 DS-GVO, da keine Rechtsgrundlage für die Weitergabe der personenbezogenen Daten vorlag.

Die Gesellschaft bzw. ehemalige Arbeitgeberin des Beschwerdeführers war hinsichtlich der Weitergabe der personenbezogenen Daten datenschutzrechtliche Verantwortliche i. S. v. Art. 4 Nr. 7 DS-GVO. Eine datenschutzrechtliche Verantwortlichkeit des Notars für die Weitergabe der personenbezogenen Daten des Beschwerdeführers an das Handelsregister liegt nicht vor, da nicht der Notar, sondern die Gesellschaft/Arbeitgeberin über die Zwecke und Mittel der Verarbeitung entschieden hat. Denn die Gesellschaft hatte die Entscheidungsbefugnis inne, welche Dokumente bzw. welche darin enthaltenen personenbezogenen Daten sie zur Anmeldung in das Handelsregister übermittelt. Die Frage, ob den Notar auch eine datenschutzrechtliche Prüfpflicht trifft, hat keine Auswirkungen auf die datenschutzrechtliche Verantwortlichkeit nach der DS-GVO im Außenverhältnis.

Die durch die Übermittlung des Gesellschafterbeschlusses erfolgte Weitergabe der personenbezogenen Daten des Beschwerdeführers bezüglich seiner Kündigung kann nicht auf eine Rechtsgrundlage gestützt werden. Insbesondere kann die Weitergabe nicht auf eine Rechtsgrundlage nach Art. 6 Abs. 1 Buchst. c DS-GVO gestützt werden.

Gemäß § 39 Abs. 2 GmbHG sind zur Anmeldung die Urkunden über die Bestellung der Geschäftsführer oder über die Beendigung der Vertretungsbefugnis in Urschrift oder in öffentlich beglaubigter Abschrift beizufügen.

Die gesetzliche Vorschrift, welche vorsieht die Urkunde über die Beendigung der Vertretungsbefugnis beizufügen, sieht nicht vor, dass hierzu die Beauftragung der Kündigung des Geschäftsführers an das Handelsregister weitergegeben werden muss.

Zur Erfüllung der Verpflichtung des § 39 Abs. 2 GmbHG standen der Verantwortlichen zwei Mittel zur Verfügung. Zum einen hatte sie die Möglichkeit einen Gesellschafterbeschluss zu fassen der sich ausschließlich auf den Widerruf der Bestellung des Beschwerdeführers als Geschäftsführer bezieht. Alternativ stand der Verantwortlichen die Möglichkeit zur Verfügung, die Teile des Gesellschafterbeschlusses, welche überobligatorische personenbezogene Daten des Beschwerdeführers enthielten, unkenntlich zu machen.

Aufgrund des vorliegenden Datenschutzverstoßes wurde die Verantwortliche gemäß Art. 58 Abs. 2 Buchst. b DS-GVO verwarnt.

PRAXISTIPP:

Achten Sie gerade bei der Weitergabe von Dokumenten zur Veröffentlichung im Handelsregister darauf, ob diese Unterlagen personenbezogene Daten enthalten, deren Veröffentlichung im Handelsregister nicht erforderlich ist. Soweit entsprechende personenbezogene Daten in den Dokumenten vorhanden sind, sollten diese unkenntlich gemacht werden. Sind die Dokumente einmal im Handelsregister veröffentlicht, kann dies irreversibel sein.

9.2 E-Mail-Postfächer ehemaliger Beschäftigter

E-Mail-Postfächer ehemaliger Beschäftigter sind schnellstens zu deaktivieren bzw. zu löschen.

Im Berichtszeitraum erreichten uns einige Beschwerden, bei denen sich ehemalige Beschäftigte darüber beschwerten, dass ihr persönliches E-Mail-Postfach beim Arbeitgeber auch nach Beendigung des Arbeitsverhältnisses nicht gelöscht oder zumindest deaktiviert wurde und insbesondere eingehende E-Mails innerhalb des Unternehmens weitergeleitet würden. Mit dieser Vorgehensweise wollten die Arbeitgeber zumeist sicherstellen, dass betriebsrelevante E-Mails, die direkt an die (ehemaligen) Beschäftigten geschickt wurden, ankommen und bearbeitet werden können. Zudem wurde vorgetragen,

dass das E-Mail-Postfach weiterhin aktiv gehalten werden müsse, um die darin befindlichen geschäftlichen E-Mails zu sichern.

Zwar kann es in Einzelfällen zulässig sein, dass ein persönliches E-Mail-Postfach auch nach Beendigung des Arbeitsverhältnisses für einen kurzen Zeitraum aktiv bleibt, damit wichtige E-Mails eingehen können und auch Kunden ein sanfter Übergang zu einem neuen Ansprechpartner ermöglicht wird. Allerdings haben wir es in den von uns bearbeiteten Verfahren als unzulässig angesehen, dass ein persönliches E-Mail-Postfach über einen Zeitraum von mehreren Monaten nach Beendigung des Beschäftigungsverhältnisses ohne Einstellung einer Abwesenheitsnotiz aktiv blieb. In diesem Fall konnte weder nachgewiesen werden, dass eine Befugnis aus Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO (Erfüllung des Arbeitsvertrages) noch aus Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zur Verarbeitung personenbezogener Daten mittels des E-Mail-Postfaches vorlag. Wegen des Verstoßes gegen den Grundsatz der Rechtmäßigkeit gem. Art. 5 Abs. 1 Buchst. a, 6 Abs. 1 DS-GVO haben wir eine Verwarnung gem. Art. 58 Abs. 2 Buchst. b DS-GVO ausgesprochen.

Der Umgang mit dem persönlichen E-Mails-Postfach sollte deshalb in einem Offboarding-Prozess/-Leitfaden geregelt werden. Dieser sollte sich insbesondere damit befassen, ob und ggf. wie lange und mit welcher Begründung ein persönliches E-Mail-Postfach eines Beschäftigten nach Beendigung des Arbeitsverhältnisses aktiv gehalten wird, wie mit den bereits im E-Mail-Postfach vorhandenen, aber auch mit neu eingehenden E-Mails umgegangen wird, wer welche Abwesenheitsnotiz einrichtet, wie mit privaten bzw. sensiblen E-Mail-Inhalten umgegangen wird und wer für die Sichtung und ggf. Ablage bzw. Weitergabe zur Bearbeitung zuständig ist. Diese Vorgehensweise sollte den Beschäftigten bereits im Vorfeld, d. h. während des bestehenden Beschäftigungsverhältnisses, transparent dargestellt werden.

9.3 GPS-Tracking in Firmenfahrzeugen

GPS-Tracker werden immer häufiger in Firmenfahrzeugen eingesetzt, sind jedoch nur in Ausnahmefällen zulässig.

Die Ortung von Beschäftigten mittels GPS-Tracker vor allem in Fahrzeugen, aber auch z. B. in Kleidungsstücken, in Arbeitsmaterialien und an einem Schlüsselbund und die damit einhergehende Datenverarbeitung war auch in diesem Berichtszeitraum Gegenstand einiger Beschwerden, Hinweise und Anfragen. Im Folgenden möchten wir deshalb die datenschutzrechtlichen Rahmenbedingungen für den Einsatz von GPS-Trackern in Fahrzeugen skizzieren:

GPS-Tracker in Fahrzeugen speichern standortbezogene Daten, sowie Zusatzinformationen wie Datum, Uhrzeit, Geschwindigkeit und gefahrene Strecke. Dabei handelt es sich zwar primär um Fahrzeugdaten, jedoch handelt es sich auch um personenbezogene Daten i. S. v. Art. 4 Nr. 1 DS-GVO, sobald die Daten einem bestimmten Fahrer zugeordnet werden können. Der jeweilige Fahrer des Fahrzeugs wird über das ihm zugeteilte Fahrzeug identifizierbar, wodurch diese Daten personenbeziehbar sind.

Nach Art. 6 Abs. 1 DS-GVO ist die Datenverarbeitung nur rechtmäßig, wenn eine der in Art. 6 Abs. 1 UAbs. 1 Buchst. a -f DS-GVO aufgezählten Befugnisse vorliegt (Grundsatz der Rechtmäßigkeit, Art. 5 Abs. 1 Buchst. a DS-GVO).

Beim Einsatz von GPS-Trackern im Beschäftigtenkontext kommen insbesondere die Befugnisse aus Art. 6 Abs. 1 UAbs. 1 Buchst. b, c und f DS-GVO in Betracht.

Die mit der GPS-Ortung einhergehende Datenverarbeitung kann grundsätzlich nicht auf eine Einwilligung gem. Art. 6 Abs. 1 UAbs. 1 Buchst. a, 7 DS-GVO, § 26 Abs. 2 BDSG gestützt werden, da es regelmäßig bereits an der Freiwilligkeit einer Einwilligung fehlt.

Ob und inwieweit die Anforderungen der Befugnisse aus Art. 6 Abs. 1 UABs. 1 Buchst. b, c oder f DS-GVO erfüllt sind, muss der Verantwortliche (im Beschäftigtenkontext i. d. R. der Arbeitgeber) im konkreten Anwendungsfall prüfen.

Dabei ist allen Befugnissen gemein, dass insbesondere die Erforderlichkeit der Datenverarbeitung (Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 Buchst. c DS-GVO) nachgewiesen werden können muss. Die Datenverarbeitung muss somit geeignet sein und es darf keine ebenso wirksamen, aber gleich gut geeignete Alternativen geben. Für die Bewertung der Erforderlichkeit spielt es dabei nicht nur eine Rolle, ob der Zweck der Datenverarbeitung mit alternativen, d. h. gänzlich anderen und milderen Mitteln erreicht werden, sondern – soweit eine Verarbeitung der Standortdaten dem Grunde nach begründbar ist – die Verarbeitung weniger invasiv gestaltet werden kann. Hierzu sind beispielsweise Überlegungen dahingehend anzustellen, ob es einer (zeitlich beschränkten) Aufzeichnung bedarf oder ein (punktueller) Echtzeitzugriff ausreicht oder ob die Verarbeitung „verwaschener" Standortdaten ausreichen kann.

Zudem muss die Datenverarbeitung immer verhältnismäßig sein. Die Datenverarbeitung muss sich daher im Ausgleich der widerstreitenden Interessen als angemessen erweisen.

Zu den benannten Befugnisnormen im Einzelnen:

Nach **Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO** ist eine Verarbeitung gestattet, wenn sie für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist (vorliegend in der Regel die Durchführung des Arbeitsvertrages), erforderlich ist. Dabei ist vorab eine eingehende Überprüfung der Erforderlichkeit notwendig. Die Rechtsprechung des EuGH verlangt diesbezüglich, dass die Datenverarbeitung objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmte Vertragsleistung ist. Der Verantwortliche muss somit nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könnte. Die Ortung eines Beschäftigten ist in einem Beschäftigungsverhältnis grundsätzlich nicht erforderlich, um den Arbeitsvertrag erfüllen zu können. Die Kontrolle der Einhaltung arbeitsrechtlicher Pflichten, wie z. B. eine Überprüfung der Einhaltung der Arbeitszeit, der Tätigkeit am vereinbarten Arbeitsort (vgl. hierzu unseren Tätigkeitsbericht 2022, Kapitel 11.2), etwaig (privater) Abweichungen von der Route rechtfertigen den Einsatz einer GPS-Ortung auf Grundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO regelmäßig nicht; Ausnahmen können allenfalls bei Vorliegen eines dokumentierten konkreten Verdachts der Begehung einer Straftat oder schwerer Pflichtverletzungen gelten, soweit die Datenverarbeitung erforderlich und verhältnismäßig ist (vgl. § 26 Abs. 1 S. 2 BDSG für den Verdacht von Straftaten bzw. entsprechend für den Verdacht schwerer Pflichtverletzungen).

Nach **Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO** ist die Verarbeitung rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung des Verantwortlichen erforderlich ist. Hierunter fällt beispielsweise die Verpflichtung eines Verantwortlichen, Aufzeichnungen über die Routen seiner Mitarbeiter zu führen, die der Lenk- und Ruhezeiten nach der Verordnung (EG) Nr. 561/2006 unterfallen. Eine Datenerhebung zur Wegstrecke - über die vom Fahrtenschreiber aufgezeichneten Daten hinaus - ist zur Erfüllung der rechtlichen Verpflichtung regelmäßig nicht erforderlich, insbesondere nicht zu dem genauen Standort sowie sämtlichen Zusatzinformationen.

Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO fordert eine Abwägung zwischen den Interessen des Verantwortlichen an der Verarbeitung und dem Interesse des Betroffenen. Die Verarbeitung ist

hiernach rechtmäßig, wenn ein berechtigtes Interesse des Verantwortlichen (hier i. d. R. des Arbeitgebers) oder eines Dritten besteht und dieses Interesse den betroffenen Personen mitgeteilt wurde, die Datenverarbeitung zur Wahrung des berechtigten Interesses erforderlich ist und nicht die Interessen oder Grundrechte oder Grundfreiheiten überwiegen.

Die berechtigten Interessen müssen tatsächlich und aktuell bestehen, d. h. es muss eine konkrete Interessenlage nachgewiesen werden können und die betroffenen Personen sind hierüber zu informieren. Die Verhinderung bzw. Verfolgung abstrakter und hypothetischer Gefährdungen oder das Interesse, Daten auf Vorrat zu sammeln stellen grundsätzlich kein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO dar. Ist ein berechtigtes Interesse gegeben, muss die Datenverarbeitung erforderlich sein, um das berechtigte Interesse wahren zu können. In der sodann durchzuführenden Interessenabwägung sind die Interessen, Grundrechte und Grundfreiheiten, die Auswirkungen der Verarbeitung auf die betroffenen Personen (Art der Daten, Kontext, Erwartungen der betroffenen Personen, Möglichkeiten der Abschwächung) gegen die berechtigten Interessen des Verantwortlichen oder des Dritten abzuwägen und müssen zugunsten des Verantwortlichen (kein Überwiegen der Interessen der betroffenen Personen) ausfallen.

Art. 21 Abs. 1 DS-GVO sieht darüber hinaus ein Widerspruchsrecht vor, soweit eine Datenverarbeitung auf Grundlage des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO erfolgt. Bringt eine betroffene Person Gründe vor, die sich aus ihrer besonderen Situation ergeben, muss eine erneute Interessenabwägung unter Einbeziehung der vorgetragenen Gründe vorgenommen werden. Nur wenn weiterhin die Interessen der widersprechenden Person nicht überwiegen, ist die Datenverarbeitung (weiterhin) zulässig. Auf das Widerspruchsrecht muss die betroffene Person gem. Art. 21 Abs. 4 DS-GVO unmissverständlich und ausdrücklich hingewiesen werden.

In begründeten Ausnahmen haben wir auf Grundlage des Art. 6 Abs.1 UAbs.1 Buchst. f DS-GVO das GPS-Tracking in Firmenfahrzeugen als zulässig erachtet.

In einem Fall wurden durch den betroffenen Arbeitnehmer Sprengstoffe und entsprechendes Zubehör mit dem LKW transportiert. Dabei wurden die mittels eines GPS-Trackers erhobenen GPS-Daten gespeichert und im konkreten Fall zur Kontrolle des Beschäftigten verarbeitet.

Die Verantwortliche teilte hierzu mit, dass sie den Einsatz der GPS-Tracker in den jeweiligen Fahrzeugen auf deren Verpflichtung zum Schutz vor Diebstahl aus dem Übereinkommen über die internationale Beförderung gefährlicher Güter auf der Straße (1.10.3.3 ADR) stütze. Zweck war hingegen nicht die Überwachung der Beschäftigten.

Vielmehr sei aufgefallen, dass der betroffene Arbeitnehmer für dieselben Strecken wesentlich längere Arbeitszeiten erfasste, als dessen Kollegen. Dies wertete die Verantwortliche als Warnzeichen für eine Gefährdungslage und entschied sich, die GPS-Daten anlassbezogen zu prüfen. Durch die Auswertung der GPS-Daten konnte festgestellt werden, dass die betroffene Person erheblich von den vorgesehenen Routen zu privaten Zwecken abgewichen war und somit eine Gefahrenlage geschaffen hatte. Sowohl das Erheben und Speichern, als auch der Zugriff auf die GPS-Daten im konkreten Einzelfall wurde im Ergebnis als datenschutzrechtlich zulässig angesehen.

Ist es dem Beschäftigten erlaubt, ein Firmenfahrzeug auch privat zu nutzen, so ist eine Standortbestimmung während der privaten Nutzung grundsätzlich ausgeschlossen. Bei einer Mischnutzung muss es dem Beschäftigten – soweit eine Ortung während er seiner Tätigkeit nachgeht zulässig ist – möglich sein, die GPS-Ortung in der Freizeit zu deaktivieren.

Selbstverständlich müssen dann, wenn Beschäftige Firmenfahrzeuge privat erwerben und nutzen, die Fahrzeuge also aus dem Betriebsvermögen entnommen werden, Datenverarbeitungen mittels Geolokalisierung durch den Arbeitgeber beendet werden.

Den Verantwortlichen trifft beim Einsatz eines GPS-Trackers und eine damit einhergehende Verarbeitung personenbezogener Daten eine Informationspflicht gemäß Art. 13 DS-GVO (**Grundsatz der Transparenz, Art. 5 Abs. 1 Buchst. a DS-GVO**). Dies bedeutet, dass insbesondere die betroffenen Beschäftigten spätestens zum Zeitpunkt der Erhebung der Beschäftigtendaten/Ortungsdaten über den Einsatz des GPS-Trackers informiert werden müssen. Informiert werden muss insbesondere über die Zwecke und Rechtsgrundlage der Datenverarbeitung. Soweit die Datenverarbeitung auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt wird, muss auch über die berechtigten Interessen sowie gem. Art. 21 Abs. 4 DS-GVO über das Widerspruchsrecht informiert werden.

Die Erfahrung zeigt, dass es äußerst ratsam ist, unmittelbar vor bzw. spätestens mit der Einführung einer GPS-Ortung die Beschäftigten transparent hierüber zu informieren. Eine Vielzahl der uns vorliegenden Eingaben und Anfragen wurde anlässlich einer fehlenden Transparenz bei uns eingelegt.

Datenschutzwidrig ist es auch, wenn – wie in einem unserer Vorgänge geschehen – eine Ortungssoftware „testweise" betrieben wird, hierbei jedoch Echtdaten von nicht informierten Beschäftigten verarbeitet werden.

Existiert bei dem Arbeitgeber ein Betriebsrat, steht diesem ohnehin gem. § 87 Abs. 1 Nr. 6 BetrVG ein Mitbestimmungsrecht zu. Da jedoch entsprechend der EuGH-Rechtsprechung zu Betriebsvereinbarungen (C-65/23) einer solchen nicht der Charakter einer alleinstehenden Befugnis zukommt, sondern sich eine solche vielmehr auf eine Befugnis gem. Art. 6 Abs. 1 DS-GVO stützen muss, ist die Rechtmäßigkeit an den oben dargelegten Anforderungen zu messen.

Die Geolokalisierung von Beschäftigten wird in Nr. 8 der Liste der Verarbeitungstätigkeiten, für die eine Datenschutzfolgeabschätzung gem. Art. 35 DS-GVO durchzuführen ist (https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf) aufgelistet, so dass eine solche vor Einsatz von Ortungsgeräten erfolgen muss.

10

Videoüberwachung

10 Videoüberwachung

10.1 Datenschutzrechtliche Anforderung beim Einsatz sog. Dashcams

Eine erhöhte Betriebsgefahr von Busunternehmen alleine rechtfertigt nicht eine mehrstündige anlasslose Speicherung von Dashcam- Aufzeichnungen.

Im Berichtszeitraum erreichte uns eine Beschwerde bezüglich des Einsatzes von Dashcams in den Omnibussen eines Reisebusunternehmens.

Im laufenden Verfahren stellte sich heraus, dass das Reisbusunternehmen in sämtlichen Omnibussen Dashcams einsetzte, welche ohne einen konkreten Anlass (z. B Auslösen eines Crashsensors) 40 Stunden in regulärer Auflösung und 60 Stunden in reduzierter Auflösung und Qualität speicherte. Die erfassten personenbezogenen Daten (Fußgänger, Kfz-Kennzeichen, etc.) wurden zwar automatisch unmittelbar verpixelt, allerdings handelte es sich nicht um eine irreversible Verpixelung, sodass die personenbezogenen Daten im Nachgang wieder erkennbar gemacht werden konnten.

Zusätzlich wurden die Aufzeichnungen nach anlassbezogener Aufforderung oder nach dem vollautomatischen Erkennen von auffälligen Fahrmanövern (z. B. bei einem Unfall) in eine Cloud hochgeladen, wobei diese Videos insgesamt 10 Sekunden – jeweils 5 Sekunden vor und nach einem Ereignis andauerten. In der Cloudplattform wurde das (anlassbezogene) Videomaterial für 6 Monate vorgehalten.

Der Einsatz der Dashcam erfolgte zum Zweck der Unfallaufklärung und Entlastung der Verantwortlichen aufgrund einer bei Omnibussen haftungsrechtlich erhöhten Betriebsgefahr, sowie der Abwehr von unbegründeten Schadensersatzansprüchen.

Eine anlasslose Speicherung der Daten von über zwei Minuten verstößt gegen den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a DS-GVO, da keine Rechtsgrundlage für die Datenverarbeitung vorliegt. Insbesondere konnte die Speicherung der personenbezogenen Daten für einen Zeitraum von über zwei Minuten nicht mit einem berechtigten Interesse der Verantwortlichen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gerechtfertigt werden.

Selbst wenn man ein berechtigtes Interesse des Verantwortlichen darin erkennen kann, dass dieser mit entsprechenden Aufzeichnungen etwaige Beweismittel im Fall eines Unfalls im Straßenverkehr oder aber zur Abwehr von (unbegründeten) Schadensersatzansprüche der Beförderungsgäste oder sonstiger Verkehrsteilnehmer, sichern möchte, rechtfertigt dieses Interesse bei der nach Art. 6 Abs. 1 Buchst. f DS-GVO gebotenen Erforderlichkeitsprüfung und Interessensabwägung nicht, die angefertigten Aufzeichnungen - ohne einen konkreten Anlass - über einen Zeitraum von mehr als zwei Minuten zu speichern.

Vielmehr ist eine entsprechend kurze Speicherung geeignet und ausreichend, um im Falle eines konkreten Anlasses eine längerfristige Dokumentation zu ermöglichen. Denn erst bei Vorliegen eines konkreten Ereignisses ist eine (längerfristige) Speicherung zur Wahrung des berechtigten Beweissicherungsinteresses (mit dem Ziel einer Strafverfolgung bzw. der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) erforderlich. Die eingesetzten Systeme müssen es deshalb ermöglichen und so eingerichtet sein, dass Aufzeichnungen erst dann, wenn konkrete (Unfall-)Ereignisse stattfinden, längerfristig zu dem dann konkreten Zweck gesichert werden. Dies kann mittels

automatischer Erkennung von konkreten Ereignissen durch z. B. einen Crash-Sensor oder aber manuell, z. B. über die Betätigung einer Taste o. ä. am Gerät oder Bordcomputer, erfolgen. Dass eine etwaig erhöhte Betriebsgefahr bzw. eine konkrete Interessenlage dahingehend, rückwirkend Aufzeichnungen auf Vorfälle hin sichten zu können, eine längere Speicherdauer erforderlich machen würde, konnte – auch vor dem Hintergrund der technischen Möglichkeiten - seitens des Verantwortlichen nicht nachgewiesen werden.

Die betroffenen Personen haben außerdem ein erheblich schutzwürdiges Interesse daran, im öffentlichen Straßenraum grundsätzlich nicht einer Videoüberwachung ihres Verhaltens unterworfen zu werden. Bei der Abwägung zwischen Beweissicherungsinteresse für den Fall eines etwaigen Unfalls und dem erheblichen legitimen Interesse der anderen Verkehrsteilnehmer, grundsätzlich nicht Gegenstand einer Videoaufzeichnung im öffentlichen Straßenverkehr zu sein, überwiegt eindeutig das letztgenannte Interesse der anderen Verkehrsteilnehmer (VG Ansbach, Urteil vom 12.08.2014 - 4 K 13.01634).

Dies ändert sich auch dann nicht, wenn die personenbezogenen Daten zwar in einem ersten Schritt unmittelbar unkenntlich gemacht werden – diese Unkenntlichmachung aber jederzeit durch die Verantwortliche nachträglich aufgehoben werden kann.

Die Verantwortliche wurde vorliegend gemäß Art. 58 Abs. 2 Buchst. f DS-GVO angewiesen es zu unterlassen, die mittels der von ihr eingesetzten Dashcam angefertigten Aufzeichnungen des öffentlichen Straßenverkehrs über eine Speicherung von zwei Minuten hinaus anlasslos zu verarbeiten.

Wann ist eine Dashcam datenschutzrechtlich zulässig?

Eine Dashcam, welche den öffentlichen Straßenverkehr erfasst ist nur dann zulässig, wenn der Ringspeicher die anlasslos gefertigten Aufzeichnungen spätestens nach zwei Minuten löscht und eine weitere Speicherung über diesen Zeitraum hinaus nur im Falle eines Anlasses (manuelles Anfordern, Crashsensor, etc.) vorgenommen wird.

Nicht jede auf dem Markt erhältliche Dashcam ermöglicht einen datenschutzkonformen Einsatz dieser Kameras. Beabsichtigen Unternehmen die Fahrzeuge Ihres Fuhrparks mit einer Dashcam auszustatten, sind diese daher angehalten die datenschutzrechtliche Zulässigkeit des Einsatzes der Dashcam zu überprüfen, gegebenenfalls etwaige Einstellungen vorzunehmen und sich nicht ausschließlich auf die Behauptungen der Hersteller oder Verkäufer entsprechender Produkte zu verlassen.

11

Gesundheit und Soziales, Versicherungen

11 Gesundheit und Soziales, Versicherungen

11.1 Online-Terminbuchungen und Terminmanagement in einer Arztpraxis

Der Einsatz von externen Unternehmen zum Zwecke der Online-Terminbuchung und des Terminmanagements durch eine Arztpraxis kann im Rahmen einer Auftragsverarbeitung nach Art. 28 DS-GVO datenschutzkonform ausgestaltet werden.

Zunehmend können Termine bei Ärztinnen und Ärzten online, bspw. auf deren Webseite gebucht werden. Hierzu werden von Arztpraxen im Regelfall externe Unternehmen im Rahmen eines Auftragsverarbeitungsvertrags eingesetzt. Damit Patientendaten bei solchen Online-Terminbuchungen und beim Terminmanagement datenschutzkonform verarbeitet werden, werden unterschiedliche Anforderungen an die Arztpraxis und das externe Unternehmen gestellt.

Generell gilt, dass nur die Daten von der Patientin bzw. dem Patienten zur Terminvereinbarung abgefragt werden dürfen, die dazu auch tatsächlich erforderlich sind, insbesondere der Name, das Geburtsdatum, die Art des Termins und eine Kontaktmöglichkeit. Beim Einsatz eines externen Unternehmens für das Terminmanagement darf im Vorfeld keine pauschale Übermittlung aller Patientenstammdaten stattfinden. Auch dürfen keine Patientendaten, die Gegenstand der Auftragsverarbeitung sind, durch das externe Unternehmen zu eigenen Zwecken weiterverarbeitet werden. Daneben sind Termineintragungen innerhalb einer kurzen Frist nach dem Termin aus dem Terminmanagementsystem zu löschen. Seitens der Arztpraxis sind zudem technisch-organisatorische Maßnahmen zu treffen, bspw. dass durch das externe Unternehmen eine ausreichende Gewähr für die Vertraulichkeit der Verarbeitung geboten wird. Werden alle Voraussetzungen erfüllt, liegt eine datenschutzkonform umgesetzte Auftragsverarbeitung gemäß Art. 28 DS-GVO vor, wobei die Arztpraxis datenschutzrechtlich Verantwortlicher ist. Eine Patientin bzw. ein Patient muss in diesem Fall keine Einwilligung in die Verarbeitung ihrer bzw. seiner Daten durch den Auftragsverarbeiter erteilen.

Für die Versendung von Terminerinnerungen ist hingegen immer eine Einwilligung nötig, da diese Benachrichtigungen nicht für den konkreten Behandlungstermin erforderlich sind.

Wird ein externes Unternehmen zum Zwecke der Online-Terminbuchung und des Terminmanagements von einer Arztpraxis beauftragt, so sind die Patientinnen und Patienten in den gemäß Art. 13 DS-GVO zur Verfügung zu stellenden Informationen zum Datenschutz darüber zu informieren, dass das externe Unternehmen Empfänger ihrer Daten ist.

Von der eben beschriebenen Online-Terminbuchung auf der Website der Arztpraxis ist eine Terminbuchung abzugrenzen, die direkt über die Plattform des externen Unternehmens vorgenommen werden kann, wobei meist ein Benutzerkonto anzulegen ist. Hier ist nicht die Arztpraxis, bei der der Temin gebucht wurde, datenschutzrechtlich Verantwortlicher, sondern das externe Unternehmen selbst.

Der aktuelle Beschluss der DSK vom 16.06.2025 zu der behandelten Thematik kann unter folgendem Link abgerufen werden: Datenschutz bei der Terminverwaltung durch Heilberufspraxen.

11.2 Löschpflicht von Gesundheitsdaten bei erfolgtem Widerruf der Einwilligung

Widerruft eine betroffene Person die zuvor erteilte Einwilligung, so hat der Verantwortliche diese Daten zu löschen.

Im Berichtszeitraum erreichte uns eine Eingabe, mit welcher sich ein Bürger bei uns beschwerte, dass trotz vorgenommenen Widerrufs der zuvor erteilten Einwilligung zur Speicherung von Gesundheitsdaten im Falle eines nicht zustande gekommen Versicherungsvertrages, keine Löschung dieser Daten durch das Versicherungsunternehmen vorgenommen wurde. Im konkreten Fall ging es um den möglichen Abschluss einer Berufsunfähigkeitsversicherung. Bei erstmaliger Antragsstellung erfolgte das Angebot aufgrund der getätigten Angaben des Bürgers zu dessen Gesundheitszustand nur auf Grundlage eines entsprechenden Risikozuschlags. Dieses Angebot lehnte der Betroffene ab und widerrief parallel die zuvor erteilte Einwilligung zur Speicherung der Gesundheitsdaten und verlangte deren Löschung. Rund ein halbes Jahr später wandte sich der Bürger erneut an die Versicherung. Diesmal ließ der Betroffene jedoch die Angaben, die bei der erstmaligen Antragsstellung zu einem Risikozuschlag geführten hatten, weg. Die Versicherung bot jedoch den Abschluss der Berufsunfähigkeitsversicherung erneut mit identischen Risikozuschlag unter Heranziehung der Gesundheitsdaten aus der erstmaligen Antragstellung an.

Durch die wirksame Ausübung des Widerrufsrecht nach Art. 7 Abs. 3 Satz 1 DS-GVO ist die Rechtsgrundlage für die Speicherung der Gesundheitsdaten aus der erstmaligen Antragstellung entfallen. Entsprechend der Leitlinien des Europäischen Datenschutzausschusses (EDSA) zur Einwilligung (vgl. EDSA Leitlinie 05/2020, dort Rn. 121 ff.) kommt bei Wegfall der Einwilligung als Rechtsgrundlage für die Datenverarbeitung auch kein Austausch von Rechtsgrundlagen in Betracht. Aus dem wirksamen Widerruf folgt eine Löschpflicht nach Art. 17 Abs. 1 Buchst. b DS-GVO. Aufgrund des eindeutigen Wortlautes der DS-GVO besteht, selbst bei Verdacht eines betrügerischen Verhaltens, keine Möglichkeit den Widerruf einer Einwilligung, wie von der Versicherung vorgetragen, nach Treu und Glauben im Wege einer teleologischen Reduktion einzuschränken. Nach Darlegung unserer Rechtsaufassung wurden die Gesundheitsdaten aus der ersten Vertragsanbahnung gelöscht und das Verfahren mit einer kostenpflichtigen Verwarnung gemäß Art. 58 Abs. 2 Buchst. b DS- GVO abgeschlossen.

Der Fall zeigt, dass hinsichtlich der Rechtsgrundlage zur Speicherung von Gesundheitsdaten, in den Fällen, in denen kein Vertrag zustande kommt, noch Nachbesserungsbedarf besteht um die Versicherungsgemeinschaft besser vor betrügerischen Handel zu schützen. Deshalb befinden sich das BayLDA sowie weitere Aufsichtsbehörden bereits im Austausch mit Vertreterinneren und Vertretern des Gesamtverbands der Deutschen Versicherungswirtschaft e.V. (GDV).

12

Rechtsanwältinnen und Rechtsanwälte

12 Rechtsanwältinnen und Rechtsanwälte

12.1 E-Mail-Kommunikation zwischen Berufsgeheimnisträgern und betroffenen Personen

Bei der Kommunikation zwischen Berufsgeheimnisträgern mit betroffenen Personen stehen die vorzuhaltenden technischen und organisatorischen Maßnahmen nicht zur Disposition der Beteiligten.

Im Berichtszeitraum hatten wir uns erneut mit Fragen zu den technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO bei der E-Mail-Kommunikation von Rechtsanwälten zu beschäftigen. Bereits in unserem Tätigkeitsbericht 2019 unter Punkt 18.5 hatten wir uns zu den generellen datenschutzrechtlichen Anforderungen an eine E-Mail-Korrespondenz zwischen Rechtsanwälten und deren Mandanten, sowie mit der Gegenseite geäußert.

Im Hinblick auf die vorzuhaltenden technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO ist zu beachten, dass sich die jeweiligen Anforderungen nach dem durch die Datenverarbeitung entstehenden Risiko für die Rechte und Freiheiten der hiervon betroffenen Personen nach dem jeweiligen Einzelfall richten. Die Tatsache, dass die per E-Mail übermittelten Daten dem Berufsgeheimnis unterliegen können, begründet nach unserer Auffassung für sich genommen noch kein hohes Risiko für die betroffene Person. In jedem Fall muss bei der Kommunikation per E-Mail eine Transportverschlüsselung angewandt werden – diese ist heutzutage in der Regel bei allen Mail-Servern bereits standardmäßig implementiert und entspricht dem aktuellen technischen Standard. Soweit besondere Kategorien personenbezogener Daten oder andere sensible Informationen übermittelt werden sollen, ist zusätzlich eine Inhaltsverschlüsselung zu gewährleisten. Eine inhaltliche Verschlüsselung kann mittels PGP oder S/MIME, oder auch durch den Versand einer kennwortgesicherten PDF-Datei mit telefonischer Passwortabfrage umgesetzt werden.

Da es sich bei den nach Art. 32 DS-GVO vorzuhaltenden Maßnahmen um objektive Rechtspflichten handelt, stehen diese grundsätzlich nicht zur Disposition der Beteiligten. Daher kann sich ein Rechtsanwalt, der eine Verarbeitung durchführt, die die Übermittlung sensibler Daten erfordert, nicht darauf zurückziehen, dass er schon grundsätzlich keine sichere Übermittlung gewährleisten kann und dem Betroffenen eine pauschale Einwilligung dazu abringen. Vielmehr hat er eine sichere Übermittlungsform bereits zum Zeitpunkt der Auswahl der Mittel für die Verarbeitung vorzuhalten.

Unter Beachtung des Selbstbestimmungsrechts der betroffenen Personen ist es jedoch möglich, dass diese in Bezug auf eine konkrete, sie betreffende Verarbeitung auf die Einhaltung des angemessenen Schutzniveaus verzichten kann. Zu den Voraussetzungen im Einzelfall verweisen wir insoweit auf den entsprechenden DSK Beschluss vom 24.11.2021 (abrufbar unter: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf).

Soweit E-Mails eines Rechtsanwaltes auch sensible personenbezogene Daten Dritter mit einem hohen Risiko (z. B. zu der gegnerischen Partei) enthalten, ist jedoch zwingend eine Inhaltsverschlüsselung vorzunehmen. Wird nun also bspw. eine vertiefte Kommunikation zur betroffenen Sache der anwaltlichen Vertretung per E-Mail geführt, ist davon auszugehen, dass diese ohne eine inhaltliche Verschlüsselung nicht ausreichend sicher ist.

In Fällen in denen ein Mandant oder die Gegenseite gegenüber dem Rechtsanwalt anzeigt, dass ein bestimmter Kommunikationsweg nicht

gewünscht ist, da die verwendete E-Mail-Adresse bspw. auch einen Zugriff durch unbefugte Dritte ermöglicht, und dem Rechtsanwalt ein gleichwertiger Kommunikationsweg zu Verfügung steht (bspw. durch Angabe einer anderen E-Mail-Adresse), kann eine weitere Verwendung der vorherigen E-Mail-Adresse nicht mehr auf. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden und deren Verarbeitung wäre damit unzulässig.

Sollte eine betroffene Person die Kommunikation per E-Mail gänzlich ablehnen, ist dies als Widerspruch nach Art. 21 DS-GVO anzusehen, welcher im Rahmen einer Interessenabwägung zu prüfen ist.

13

Digitalwirtschaft

13 Digitalwirtschaft

13.1 Transkription von Videokonferenzen

Nicht nur mit Einwilligung möglich.

Im Berichtszeitraum erreichten das BayLDA vermehrt Anfragen von Verantwortlichen zur datenschutzkonformen Transkription von Videokonferenzen. Hintergrund war insbesondere die zunehmende Integration entsprechender Funktionen in gängige Videokonferenzsysteme, sowie der Einsatz externer Sprach-zu-Text-Dienste.

Die Anfragen betrafen vor allem Fragen zur geeigneten Rechtsgrundlage, sowie zu den Rechten der betroffenen Personen. In mehreren Fällen bestanden zudem Unsicherheiten im Hinblick auf den Umgang mit sensiblen Gesprächsinhalten.

Die automatisierte Transkription stellt eine Verarbeitung personenbezogener Daten dar, da das gesprochene Wort technisch erfasst und in Textform überführt wird. Dies gilt unabhängig davon, ob zusätzlich eine dauerhafte Audio- oder Videoaufzeichnung gespeichert wird. Auch bei rein textbasierter Transkription ist regelmäßig eine zumindest kurzzeitige Audioverarbeitung technisch erforderlich.

Damit ist eine Rechtsgrundlage entsprechend Art. 6 DS-GVO erforderlich. In vielen Konstellationen, gerade im Beschäftigtenkontext wurde die Einwilligung als nicht praxisgerecht betrachtet, da Zweifel an der Freiwilligkeit bestehen können. Die Vertragsgrundlage ist in diesen Fällen auch zumeist nicht geeignet, sodass wir in diesem Zusammenhang vor allem Fragestellungen zur Rechtsgrundlage des berechtigten Interesses zu beantworten hatten. Voraussetzung für die Heranziehung von Art. 6 Abs. 1 Buchst. f DS-GVO ist eine nachvollziehbare Interessenabwägung, in der insbesondere Zweck, Erforderlichkeit und die Interessen der betroffenen Personen zu berücksichtigen sind.

Im Rahmen der Erforderlichkeitsprüfung wurde darauf hingewiesen, dass eine pauschale oder dauerhafte Aktivierung von Transkriptionsfunktionen regelmäßig nicht geboten ist. Verantwortliche haben zu prüfen, ob der jeweilige Zweck auch durch weniger eingriffsintensive Mittel, etwa durch Ergebnisprotokolle oder manuelle Mitschriften, erreicht werden kann. In bestimmten Konstellationen, etwa bei langen und komplexen Besprechungen, in internationalen Teams oder zur Unterstützung barrierefreier Teilnahme, können solche Alternativen jedoch nicht gleich wirksam sein.

Besondere Bedeutung kommt auch der technischen Ausgestaltung der Transkription zu. Als datensparsame Ausprägung wurde insbesondere der Einsatz von Live-Untertiteln ohne dauerhafte Speicherung, sowie technische und organisatorische Maßnahmen hervorgehoben. Weitergehende Analyse- oder Auswertungsfunktionen sollten kritisch geprüft und gegebenenfalls deaktiviert werden.

Mehrere Anfragen betrafen zudem die Ausübung von Widerspruchsrechten nach Art. 21 DS-GVO. Verantwortliche müssen sicherstellen, dass ein Widerspruch gegen die Transkription praktisch wirksam ausgeübt werden kann. Erfolgt ein Widerspruch während einer laufenden Transkription, ist die Verarbeitung personenbezogener Daten der widersprechenden Person ab diesem Zeitpunkt zu unterlassen. Bereits rechtmäßig erfasste Inhalte sind gegebenenfalls aus dem Transkript zu entfernen oder zu anonymisieren.

Darüber hinaus kam bei einigen Anfragen auch die Frage auf, ob die oben dargestellte technisch zwingend erforderliche Aufzeichnung der

Stimme eine Verarbeitung besonderer Kategorien personenbezogener Daten entsprechend Art. 9 Abs. 1 DS-GVO darstellt. Dies ist im Regelfall zu verneinen, da die Stimme zwar als biometrisches Datum nach Art. 4 Nr. 14 DS-GVO einzuordnen ist, bei der Transkription aber regelmäßig nicht zur eindeutigen Identifizierung einer natürlichen Person eingesetzt wird. Die bei der automatisierten Transkription erfolgende Sprechertrennung erfolgt grundsätzlich über sog. Voice embeddings, also nummerische Vektoren und über externe Kontextinformationen wie bspw. das verwendete Nutzerkonto oder den aktiven Mikrofoneingang. Eine Identifizierung der sprechenden Person ist hierfür nicht notwendig.

Schließlich wurde auf den Umgang mit sensiblen Gesprächsinhalten hingewiesen. Auch wenn die Transkription nicht auf die Verarbeitung besonderer Kategorien personenbezogener Daten gerichtet ist, können solche Daten im Gesprächsverlauf inzident anfallen. In diesen Fällen sind die betreffenden Passagen unverzüglich zu bereinigen und von einer weiteren Nutzung auszuschließen.

Die Beratungsanfragen zeigen, dass der Einsatz von Transkriptionsfunktionen bei Videokonferenzen einer sorgfältigen datenschutzrechtlichen Bewertung bedarf. Maßgeblich ist dabei die konkrete Ausgestaltung der Verarbeitung, insbesondere im Hinblick auf Zweckbindung, Datenminimierung, Transparenz und die Wahrung der Betroffenenrechte.

13.2 Kein Anspruch auf Freischaltung eines gesperrten Online-Accounts nach Art. 15 DS-GVO

Das Auskunftsrecht nach Art. 15 DS-GVO vermittelt keinen Anspruch auf (Wieder-) Zugang zu einem gesperrten Online-Account. Es besteht lediglich ein Anspruch auf Auskunft und – auf Antrag – auf Erhalt einer Kopie der verarbeiteten personenbezogenen Daten.

Im Berichtszeitraum erreichte uns eine Vielzahl von Beschwerden im Zusammenhang mit der Sperrung von Online-Accounts (z. B. Kundenkonten bei Plattformen oder Online-Händlern).

Den Eingaben lag regelmäßig folgender Sachverhalt zugrunde:

Der Online-Account der betroffenen Person war durch den jeweiligen Anbieter gesperrt worden, sodass ein Zugriff auf das Nutzerkonto und die darin gespeicherten Daten nicht mehr möglich war. In der Regel hatte der Anbieter die betroffene Person über die Sperrung und deren Gründe (etwa Verstöße gegen Nutzungsbedingungen oder sicherheitsrelevante Auffälligkeiten) informiert. Eine Freischaltung des Accounts konnte jedoch nicht erreicht werden. Die betroffenen Personen wandten sich daraufhin an uns mit der Begründung, die Sperrung sei unrechtmäßig und verletze ihr Recht auf Auskunft nach Art. 15 DS-GVO, da sie keinen Zugriff mehr auf „ihre Daten“ hätten. Ziel war es häufig, über ein datenschutzrechtliches Verfahren die Wiederfreischaltung des Accounts zu erreichen.

Wir haben hierzu klargestellt:

Die Frage, ob ein Online-Account rechtmäßig gesperrt wurde, ist grundsätzlich keine datenschutzrechtliche Fragestellung. Maßgeblich sind insoweit die vertraglichen Vereinbarungen zwischen Anbieter und Nutzer, insbesondere die Nutzungsbedingungen. Die Prüfung der Rechtmäßigkeit einer Kontosperrung erfolgt daher nach zivilrechtlichen Maßstäben und nicht im Rahmen der datenschutzrechtlichen Aufsicht.

Ein Anspruch auf Zugang zu einem gesperrten Account lässt sich aus Art. 15 DS-GVO nicht ableiten. Das Auskunftsrecht gewährt keinen Anspruch auf Nutzung oder technische Zugriffsmöglichkeit auf ein Kundenkonto.

Art. 15 DS-GVO vermittelt vielmehr:

- das Recht auf Auskunft, ob personenbezogene Daten verarbeitet werden,
- das Recht auf Auskunft über diese personenbezogenen Daten sowie
- nach Art. 15 Abs. 3 DS-GVO das Recht, eine Kopie der personenbezogenen Daten zu erhalten, die Gegenstand der Verarbeitung sind.

Der Anspruch auf „Kopie" bedeutet dabei nicht, dass der Verantwortliche den gesperrten Account wieder freischalten oder einen vollständigen Systemzugang einräumen muss. Vielmehr ist eine Kopie der konkret verarbeiteten personenbezogenen Daten in geeigneter Form bereitzustellen (z. B. als strukturierte Datei oder Dokument).

Nicht umfasst ist ein Anspruch auf:

- Zugriff auf interne Systeme,
- Wiederherstellung der technischen Nutzungsmöglichkeit eines Accounts,
- Herausgabe von Geschäftsgeheimnissen, internen Bewertungen oder nicht personenbezogenen Daten.

Die Kopie muss die personenbezogenen Daten enthalten, die tatsächlich verarbeitet werden. Sie kann jedoch in einer anderen Form als dem ursprünglichen Account-Zugang zur Verfügung gestellt werden. Die Wahl des technischen Übermittlungswegs bleibt dem Verantwortlichen überlassen, sofern die gesetzlichen Anforderungen eingehalten werden.

Ein weiterer wichtiger Aspekt, der in diesem Zusammenhang auch oftmals aufgetreten ist, ist die Frage, warum der jeweilige Account überhaupt gesperrt wurde. Dies Information unterliegt oftmals jedoch internen Bewertungen bzw. basiert auf Geschäftsgeheimnissen. Die Offenlegung welche Art von Betrugserkennungssoftware verwendet wird, bzw. bei Online- Spielen welche Anti- Cheat- Systeme eingesetzt werden und warum diese im konkreten Fall ausschlagen ist daher regelmäßig nicht vom Auskunftsersuchen umfasst.

In einem Großteil der bei uns eingegangenen Zuschriften war ein formelles Auskunftsersuchen nach Art. 15 DS-GVO gegenüber dem Anbieter im Übrigen noch gar nicht gestellt worden. Wir haben die betroffenen Personen daher zunächst auf die Möglichkeit hingewiesen, ihr Auskunftsrecht unmittelbar gegenüber dem Verantwortlichen geltend zu machen.

13.3 Entscheidungen zum Auskunftsrecht im Onlinehandel

Beschwerden zum Auskunftsrecht nach Art. 15 DS-GVO im Onlinehandel sind unbegründet, wenn die Auskunft vollständig und in geeigneter elektronischer Form erteilt wurde, Geschäftsgeheimnisse – etwa zu Betrugsprüfungen – geschützt bleiben oder Daten Dritter durch den Verantwortlichen nicht offengelegt werden.

Wie auch in den letzten Jahren ging bei uns eine Vielzahl von Beschwerden hinsichtlich der Gewährleistung und Ausgestaltung des Auskunftsrechts nach Art. 15 DS-GVO im Bereich Onlinehandel ein. Bei einem Großteil dieser Eingaben waren grenzüberschreitende Verarbeitungen betroffen, sodass diese Verfahren im Rahmen des Kooperationsverfahrens entsprechend Artt. 60 ff. bearbeitet wurden. Eine Vielzahl dieser Verfahren konnte im Berichtszeitraum abgeschlossen werden und damit auch einige wiederkehrende Fragestellungen in Zusammenarbeit mit der in vielen Fällen federführenden luxemburgischen Aufsichtsbehörde entschieden werden.

Dazu gehörten unter anderem Beschwerden über abgelehnte oder nicht veröffentlichte Produktbewertungen. In diesen Fällen wollten betroffene Personen im Wege des Auskunftsrechts

mitgeteilt bekommen, auf welcher Grundlage die Entscheidung durch den Onlinehändler getroffen worden war, da zumeist nur ein Hinweis auf einen Verstoß gegen die entsprechenden Unternehmens- Richtlinien erfolgt war. In den vorliegenden Verfahren wurde dies als ausreichend erachtet, da eine weitergehende Offenlegung der internen Mechanismen zur Betrugsbekämpfung deren Integrität gefährdet und internen Bewertungen bzw. Geschäftsgeheimnissen unterliegt. In Abwägung nach Art. 15 Abs. 4 DS-GVO war das Unternehmen daher berechtigt, die bereitgestellten Informationen auf solche zu beschränken, die Dritten nicht ermöglichen würden, das Überwachungs- und Durchsetzungssystem zu umgehen.

Ein Großteil der Beschwerden betraf auch die Vollständigkeit der mitgeteilten Auskunft. In vielen Fällen wurde pauschal und ohne Begründung oder ersichtliche Anhaltspunkte die Vollständigkeit der Auskunftserteilung gerügt. In diesen Fällen wurden die Beschwerden als unbegründet abgewiesen, wenn der Verantwortliche die Vollständigkeit der Auskunft versichert hat und sich keine Anhaltspunkte dafür ergeben haben, dass dies unzutreffend wäre. Weiterhin stellte auch die Frage nach der Form der Auskunftserteilung einen Schwerpunkt in den Verfahren im Bereich Online- Handel dar. In mehreren verschiedenen Verfahren wurde kein Verstoß des Verantwortlichen angenommen, wenn die elektronische Bereitstellung der Auskünfte in maschinenlesbaren Formaten wie Excel, CSV oder ZIP-Dateien erfolgte. Die Anforderungen des Art. 15 Abs. 3 DS-GVO wurden hier als erfüllt angesehen, da die genannten Formate grundsätzlich geeignet, gut zugänglich und nachvollziehbar seien. Die Bereitstellung leerer Dateien auf Anfrage wurde in diesem Zusammenhang als Negativauskunft gewertet. Die Tatsache, dass solche Dateien nicht oder nur schwer ausdruckbar sind, widerspricht dem nicht, da dies keine Anforderung des Art. 15 Abs. 3 DS-GVO darstellt. In diesen Fällen ist es daher auch möglich, dass eine postalische Bereitstellung bestimmter Auskünfte verweigert werden kann.

Ein weiterer Schwerpunkt betraf sogenannte Clickstream-Daten. Die luxemburgische Aufsichtsbehörde stellte klar, dass die Auskunft auch dann vollständig ist, wenn sämtliche relevanten Browsing- und Suchdaten tatsächlich übermittelt wurden, selbst wenn diese nicht ausdrücklich als „Clickstream-Daten" bezeichnet waren.

Schließlich wurden auch Fälle von Identitätsdiebstahl bei Onlinebestellungen behandelt, bei denen unbekannte Dritte böswillig die Zahlungsmethode eines Kunden verwendeten. Die betroffenen Personen wollten im Rahmen des Auskunftsersuchens die Identität des Täters ermitteln und legten Beschwerde ein, da der Verantwortliche die Herausgabe dieser Information verweigerte.

Nutzt eine Person Zahlungsdaten einer anderen Person in einem auf seinen eigenen Namen laufenden Account, besteht ein Auskunftsanspruch des Opfers hinsichtlich aller Daten, die dem Opfer aufgrund von Inhalt, Zweck oder Wirkung der Verarbeitung zugeordnet werden können. Hierzu zählen insbesondere Zahlungs- und Transaktionsdaten, Bestell- und Rechnungsinformationen sowie interne Vorgangs- und Betrugsvermerke (siehe hierzu: Leitlinien 01/2022 des Europäischen Datenschutzausschusses zu den Rechten der betroffenen Person – Auskunftsrecht, Rn.107f.).

Kein Anspruch besteht hingegen auf Offenlegung der Identität des Accountinhabers. Der Name oder die Anschrift des Unbekannten stellen personenbezogene Daten eines Dritten dar und sind nicht erforderlich, um die Verarbeitung der personenbezogenen Daten des Opfers zu verstehen oder zu überprüfen. Art. 15 DS-GVO dient nicht der Ermittlung weiterer Verantwortlicher. Diese Auslegung steht auch im Einklang mit den Leitlinien 01/2022 des Europäischen Datenschutzausschusses, hier heißt es in Rn. 104:

"Es gibt auch Situationen, in denen die Daten nicht mit der Person, die das Auskunftsrecht ausübt, sondern mit einer anderen Person in Verbindung stehen. Die betroffene Person hat jedoch nur Anspruch auf personenbezogene Daten, die sich auf sie selbst beziehen. Daten, die ausschließlich eine andere Person betreffen, sind von diesem Anspruch ausgeschlossen"

Dies mag auf den ersten Blick unbillig erscheinen, jedoch dient das Auskunftsrecht nach Art. 15 DS-GVO dazu, die Verarbeitung personenbezogener Daten durch den Verantwortlichen (in diesen Fällen dem Onlinehändler) zu prüfen und nicht der Strafverfolgung. Betroffene Personen können über die Strafverfolgungsbehörden eine Offenlegung der Identität erreichen, da der Täter nicht durch das Datenschutzrecht vor der Strafverfolgung geschützt wird.

Anders verhält es sich hingegen in Fällen, in denen von Dritten ein Account mit dem Namen der betroffenen Person angelegt wird. In diesen Fällen sind alle Daten des Benutzerkontos (auch) personenbezogene Daten des Opfers und daher zu beauskunften.

Dies bestätigte auch das VG Berlin in seiner Entscheidung vom 09.10.2025 (Az. 1 K 463/22)

„…Sämtliche dieser Informationen sind mit der Person des Beschwerdeführers verknüpft worden, weil sie zu dem unter seinem Namen erstellten Benutzerkonto gespeichert und damit verarbeitet wurden (…). Es handelt sich daher (auch) um personenbezogene Daten des Beschwerdeführers. Darauf, dass der Beschwerdeführer diese Daten nicht selbst erzeugt bzw. zur Verfügung gestellt hat, kommt es nicht an. Es genügt für die Auskunftspflicht, dass die Klägerin die durch eine dritte Person übermittelten Daten im Sinne von Art. 4 Nr. 2 DSGVO verarbeitet hat…"

Es ist daher in diesen Konstellationen zu prüfen, welche Daten personenbezogene Daten der betroffenen Person darstellen und welche einem Dritten zuzuordnen sind und daher nicht vom Auskunftsverlangen nach Art. 15 DS-GVO umfasst sind.

13.4 Geltungsbeginn des DataAct

Erste Beratungsanfragen zum Zusammenspiel Data- Act und DS-GVO.

Mit der „Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung", kurz die „Daten-Verordnung" bzw. dem Data Act, hat die Europäische Union einen zentralen Baustein ihrer europäischen Datenstrategie geschaffen. Ziel der Verordnung ist es, den Zugang zu und die Nutzung von Daten aus vernetzten Produkten und verbundenen Diensten zu erleichtern und damit Innovation sowie neue datenbasierte Geschäftsmodelle zu fördern. Insbesondere sollen Nutzende vernetzter Produkte – etwa aus dem Bereich Industrie-4.0-Anwendungen, Smart-Home-Geräten oder vernetzten Fahrzeugen – künftig leichter auf die bei der Nutzung entstehenden Daten zugreifen und diese auch an Dritte weitergeben können.

Wesentliche Teile des Data Act gelten seit dem 12. September 2025. Der Rechtsakt enthält insbesondere Regelungen zu Datenzugangsansprüchen, zur Weitergabe von Daten an Dritte sowie zu fairen Vertragsbedingungen beim Datenzugang. Der Data Act erfasst dabei sowohl personenbezogene als auch nicht-personenbezogene Daten.

Soweit personenbezogene Daten betroffen sind, gilt jedoch weiterhin der Vorrang der Datenschutz-Grundverordnung. Datenzugangs- oder Datenweitergabepflichten nach dem Data Act dürfen daher nur umgesetzt werden, wenn zugleich die Anforderungen der DS-GVO eingehalten werden. Insbesondere bedarf jede Verarbeitung oder Übermittlung personenbezogener

Daten weiterhin einer entsprechenden datenschutzrechtlichen Rechtsgrundlage und muss die allgemeinen Grundsätze der Datenverarbeitung beachten.

Der europäische Gesetzgeber hat daher vorgesehen, dass im Bereich personenbezogener Daten grundsätzlich die bereits nach der DS-GVO zuständigen Datenschutzaufsichtsbehörden auch für die Überwachung der entsprechenden Bestimmungen des Data Act zuständig sind. In Bayern ist daher bislang das Bayerisches Landesamt für Datenschutzaufsicht für die Durchsetzung der Vorschriften des Data Act verantwortlich, soweit personenbezogene Daten betroffen sind.

Bereits zu Beginn des Berichtszeitraums, also vor Geltungsbeginn des Data Act, erreichten das BayLDA erste Beratungsanfragen von Unternehmen und Verbänden zum neuen Rechtsrahmen. In der Praxis standen dabei insbesondere Fragen zum Zusammenspiel zwischen Data Act und DS-GVO im Mittelpunkt. Häufig ging es zunächst um die grundlegende Einordnung, ob die jeweils betroffenen Daten überhaupt personenbezogene Daten im Sinne der DS-GVO darstellen oder ob es sich um rein technische bzw. nicht-personenbezogene Daten handelt.

Darüber hinaus wurde vielfach nach der datenschutzrechtlichen Rechtsgrundlage für eine Datenweitergabe gefragt, wenn ein Datenzugangsanspruch nach dem Data Act geltend gemacht wird. In diesen Fällen ist zu prüfen, ob und auf welcher Grundlage eine Verarbeitung nach der DS-GVO zulässig ist. Der Data Act selbst schafft insoweit keine eigenständige datenschutzrechtliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten.

Die bisherigen Anfragen zeigen, dass der Data Act in der Praxis häufig eine Abgrenzungs- und Koordinierungsfrage zwischen Datenzugangsrecht und Datenschutzrecht aufwirft. Das BayLDA begleitet diese Entwicklung durch Beratung und Aufsicht, um eine rechtskonforme Umsetzung der neuen europäischen Regelungen zu unterstützen.

Die Bundesregierung hat am 01.12.2025 den Entwurf eines Gesetzes zur Durchführung des Data Act in den Bundestag eingebracht (BT- Drs. 21//2998). Der zum Redaktionsschluss noch nicht verabschiedete Gesetzentwurf, sieht, für den nicht-öffentlichen Bereich eine Übertragung der Zuständigkeiten auf die Bundesnetzagentur und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vor. In diesem Fall entfällt zukünftig die Zuständigkeit des BayLDA für den DataAct, jedoch werden wir auch weiterhin einen engen Austausch mit den zuständigen Behörden anstreben, damit bspw. die Frage „ob" ein Datum personenbezogen ist, nicht für DS-GVO- Fälle anders beantwortet wird als im Lichte des DataAct.

13.5 Political Targeting

Erste Beschwerden nach der neuen EU-Verordnung über die Transparenz und das Targeting politischer Werbung.

Die Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO) ist am 13.03.2024 in Kraft getreten und ab dem 10. Oktober 2025 EU-weit verbindlich anzuwenden. Die TTPW-VO ist unmittelbar geltendes Recht und muss nur insoweit mit nationalen Durchführungsbestimmungen umgesetzt werden, als bestimmte in der EU-Verordnung vorgesehene Zuständigkeiten und Befugnisse zugewiesen werden müssen. Das hierfür geplante Durchführungsgesetz „Politische Werbung Transparenz Gesetz" (PWTG) befindet sich zum Zeitpunkt des Redaktionsschlusses noch im Gesetzgebungsprozess.

Mit der Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung hat die Europäische Union einen neuen Rechtsrahmen für politische Werbung geschaffen. Als politische Werbung im Sinne der Ver-

ordnung gelten in der Regel entgeltliche Werbebotschaften, die darauf abzielen und dazu geeignet sind, politische Prozesse wie beispielsweise Wahlen zu beeinflussen.

Ziel der Verordnung ist es insbesondere, die Transparenz politischer Online-Werbung zu erhöhen, unzulässige Targeting- und Profilingverfahren zu begrenzen und damit die informationelle Selbstbestimmung der Bürgerinnen und Bürger im politischen Meinungsbildungsprozess zu stärken.

Nach der Verordnung kommt den Datenschutzaufsichtsbehörden eine zentrale Rolle bei der Überwachung der datenschutzrechtlichen Vorgaben für politische Werbung zu. Zu den wesentlichen Aufgaben gehören insbesondere die Kontrolle der Vorschriften über

- Targeting- und Anzeigenschaltungsverfahren bei politischer Werbung (Art. 18 TTPW-VO) sowie
- die Transparenzanforderungen für politische Werbeanzeigen (Art. 19 TTPW-VO).

Damit erweitert sich der Aufgabenbereich BayLDA um die datenschutzrechtliche Kontrolle entsprechender Verfahren im Bereich politischer Online-Werbung, wobei die datenschutzrechtlichen Vorgaben der TTPW-VO die bereits bestehenden Anforderungen der DS-GVO ergänzen. Bei Verstößen gegen die TTPW-VO stehen den zuständigen Aufsichtsbehörden die in Art. 58 DS-GVO vorgesehenen Untersuchungs- und Abhilfebefugnisse sowie die Möglichkeit zur Verhängung von Geldbußen zur Verfügung

Die Nutzung personenbezogener Daten für Targeting- oder Anzeigenschaltungsverfahren im Zusammenhang mit politischer Werbung ist nach der Verordnung nur unter engen Voraussetzungen zulässig. Insbesondere ist erforderlich, dass die betroffene Person ausdrücklich in die Verarbeitung ihrer personenbezogenen Daten zu Zwecken politischer Werbung eingewilligt hat und dass die hierfür verwendeten Daten unmittelbar bei der betroffenen Person erhoben wurden.

Besonders strenge Anforderungen gelten für die Verwendung besonderer Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO, etwa Daten über politische Meinungen, religiöse Überzeugungen oder die ethnische Herkunft. Deren Verarbeitung zu Zwecken politischer Werbung ist grundsätzlich unzulässig.

Die Verordnung verpflichtet Anbieter politischer Werbung außerdem, jeder Werbeanzeige klare und leicht zugängliche Transparenzinformationen beizufügen. Dazu gehören insbesondere Angaben zum verantwortlichen politischen Akteur, zur Finanzierung der Werbung sowie zu den eingesetzten Targeting-Kriterien.

Betroffene können sich an die zuständige Datenschutzaufsichtsbehörde wenden, wenn sie den Eindruck haben, dass ihnen politische Werbung unter Einsatz unzulässiger Targeting- oder Profilingverfahren angezeigt wurde oder die vorgeschriebenen Transparenzangaben fehlen.

Im Berichtszeitraum sind bereits erste Beschwerden, die sich explizit auf die Verordnung beziehen, bei uns eingegangen; wir gehen aufgrund der bevorstehenden Kommunalwahl in Bayern von einem Anstieg der Beschwerdeeingänge im 1. Quartal 2026 aus. Die bereits abgeschlossenen Verfahren haben keine Verstöße ergeben, zum Zeitpunkt der Erstellung dieses Berichts waren aber noch nicht alle Verfahren abgeschlossen.

14

Internationaler Datenverkehr

14 Internationaler Datenverkehr

14.1 Beratungsanfragen zum EU-U.S. Data Privacy Framework

Weiterhin kein gemeinsames Verständnis von HR- Daten.

Auch im Jahr 2025 erreichten uns zahlreiche Beratungsanfragen zum EU-U.S.-Data Privacy-Framework-Angemessenheitsbeschluss der Europäischen Kommission betreffend die Übermittlung personenbezogener Daten in die USA.

Zu einigen klassischen Fragen, die uns zum EU-US-Data Privacy Framework (DPF) und zu Datenübermittlungen in die USA gestellt werden, hatten wir uns schon in vorangegangenen Tätigkeitsberichten geäußert, darunter etwa zum Verhältnis zwischen dem DPF und Standarddatenschutzklauseln oder zur Notwendigkeit der Durchführung eines „Transfer Impact Assessment" bei Übermittlungen in die USA, die nicht auf den DPF gestützt werden, sondern etwa auf die Standardvertragsklauseln der Europäischen Kommission vom 04.06.2021. Diese Fragen standen auch weiterhin im Fokus, was ihre hohe Praxisrelevanz für Daten exportierende Stellen belegt; wir konnten aber Fragen zu diesen „Dauerbrennern" in der Regel durch Verweis auf die Aussagen zum DPF aus unserem 13. Tätigkeitsbericht für das Jahr 2023 (dort Ziff. 15) klären.

Vielen Anwendern wurde zudem offenbar erst in letzter Zeit das Problem der sog. HR-Data-Zertifizierung unter dem DPF bewusst. Wie schon in unserem 14. Tätigkeitsbericht (2024) berichtet (dort Nr. 13.1) gibt es bedauerlicherweise auch weiterhin noch kein gemeinsames Verständnis der US- und der europäischen Seite zum Begriff der HR Data, wie er im DPF Verwendung findet. Dies ist misslich, weil es unter dem DPF zwei unterschiedliche Typen von Zertifizierungen auf Seiten der zertifizierungswilligen US-Unternehmen gibt: HR Data und Non-HR Data. Die beiden Zertifizierungen bezeichnen unterschiedliche Kategorien von Daten, je nach Gruppe der betroffenen Personen. US-Unternehmen können wählen, ob sie sich nur für eine der Datenkategorien oder aber für beide zertifizieren. Der Typus der Zertifizierung ist beim jeweiligen Unternehmen in der vom US-Handelsministerium geführten, online verfügbaren Liste der zertifizierten US-Unternehmen (https://www.dataprivacyframework.gov/list) angegeben. Die Datenschutzbehörden der EU-Mitgliedstaaten vertreten auch weiterhin die Auffassung, dass der Begriff HR Data aus europäischer Perspektive zu verstehen ist, so dass das empfangende US-Unternehmen grundsätzlich eine HR-Data-Zertifizierung benötigt, wenn dorthin Daten von europäischen Beschäftigten (insbesondere etwa des übermittelnden Unternehmens) auf Grundlage des DPF übermittelt werden. Die europäischen Aufsichtsbehörden – so auch unser Haus - wenden dieses Begriffsverständnis in ihrer aufsichtlichen Praxis an, sodass etwa ein bayerisches Unternehmen, welches Daten eigener Beschäftigter an einen US-Cloud-Dienstleister auf Grundlage des DPF übermitteln möchte, darauf achten muss, dass das US-Unternehmen grundsätzlich (siehe aber die nachfolgenden Ausführungen) eine HR-Data-Zertifizierung besitzt.

Der entscheidende Unterschied zwischen den beiden Zertifizierungstypen „HR Data" und „Non HR Data" liegt darin, dass sich US-Unternehmen mit HR-Data-Zertifizierung verpflichten, direkt mit den Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten zusammenzuarbeiten. Der Europäische Datenschutzausschuss hat kürzlich vor diesem Hintergrund erklärt, dass Daten von europäischen Beschäftigten auch an US-Unternehmen übermittelt werden dürfen, die nur eine Non-HR-Data-Zertifizierung besitzen, sofern sich das Unternehmen in seiner Datenschutz-Policy (Privacy Policy) verpflichtet, mit den europäischen Datenschutzaufsichtsbehörden zusammenzuarbeiten (so die kürzlich

überarbeiteten FAQ des EDSA für europäische Unternehmen zum DPF, veröffentlicht etwa auf der Website des EDSA unter https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_en). Nichtsdestotrotz ist es aus Sicht der Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten wichtig, dass die Europäische Kommission und die Aufsichtsbehörden ihre Gespräche mit der US-Seite mit dem Ziel eines gemeinsamen Verständnisses des Begriffs HR Data fortsetzen, um die Handhabung in der Praxis zu erleichtern und Fehlvorstellungen über die Reichweite des Begriffs zu vermeiden.

Anlass für weitere Anfragen zum DPF bot in den letzten Monaten des Jahres darüber hinaus das Urteil des Europäischen Gerichts erster Instanz (EuG) in der Rechtssache T-553 (Latombe ./. Europäische Kommission) vom 03.09.2025. Zugrunde lag eine Klage eines französischen Abgeordneten, mit der die Gültigkeit des Angemessenheitsbeschlusses in Frage gestellt worden war. Das Gericht bestätigte die Gültigkeit des Kommissionsbeschlusses, so dass der DPF jedenfalls vorerst weiterhin als datenschutzrechtliche Grundlage für die Übermittlung personenbezogene Daten an zertifizierte US-Unternehmen Verwendung finden kann. Allerdings hat der Kläger Rechtsmittel gegen diese Entscheidung eingelegt, sodass schließlich der Europäische Gerichtshof in letzter Instanz über die Rechtswirksamkeit des Angemessenheitsbeschlusses entscheiden wird. Hierzu Prognosen abzugeben erscheint schwierig. Es ist nachvollziehbar, dass Unternehmen und andere Daten exportierende Stellen vor diesem Hintergrund einen Mangel an Rechtssicherheit bezogen auf die Übermittlung personenbezogener Daten in die USA beklagen. Eine mögliche Lösung mag darin liegen, für Übermittlungen an DPF-zertifizierte Unternehmen eine Art „doppelten Boden" zu verwenden, indem vorsorglich für den etwaigen Wegfall des Angemessenheitsbeschlusses zum DPF mit dem Datenempfänger auch die Standardvertragsklauseln der Europäischen Kommission vom 04.06.2021 abgeschlossen werden, wobei dies nur unter der (Rechts-)Bedingung erfolgen kann, dass der DPF nachträglich wegfällt (siehe unseren 13. Tätigkeitsbericht, 2023, Ziff. 15.3). Allerdings liefert auch ein solcher vorsorglicher Abschluss von Standardvertragsklausel keine „absolute" dauerhafte Rechtssicherheit für den Fall einer etwaigen Aufhebung des DPF, da es entscheidend darauf ankommen würde, aus welchen rechtlichen Gründen etwa der DPF ggf. vom EuGH für ungültig erklärt werden würden. Solche Gründe können je nach ihrer Eigenart u. U. auch auf Übermittlungen auf Grundlage von Standardvertragsklauseln durchschlagen; so würden etwa Mängel bezogen auf den nach europäischem Recht zu verlangenden Mindestschutz in einem Drittland gegenüber staatlichen Datenzugriffen (etwa unzureichender Rechtsschutz oder Mängel bezogen auf die Verhältnismäßigkeit von Datenzugriffen) grundsätzlich auf alle Datentransfers in das betreffende Drittland durchschlagen, d. h. unabhängig vom verwendeten datenschutzrechtlichen Transfer-Instrument. Es gilt daher auch weiterhin die Entwicklungen abzuwarten.

14.2 Datenübermittlung durch Tiktok nach China

Bei Drittlandtransfers ist es Aufgabe des Datenexporteurs nachzuweisen, dass für die übermittelten Daten ein mit dem EU-Schutzniveau in der Sache gleichwertiger Schutz gewährleistet ist; verbleibende signifikante Zweifel gehen zu Lasten des Datenexporteurs.

Erhebliche öffentliche Resonanz hatte eine Entscheidung der irischen Datenschutzaufsichtsbehörde vom 30.04.2025 zum chinesischen Unternehmen TikTok hervorgerufen (Volltext in englischer Sprache veröffentlicht auf der Website der irischen Aufsichtsbehörde unter https://www.dataprotection.ie/en/treoir-

ccs/law/decisions/inquiry-tiktok-technology-limited-april-2025). Die Entscheidung erging im DS-GVO-Kooperationsverfahren, unter anderem auch mit Beteiligung der deutschen Aufsichtsbehörden. Bemerkenswert ist der Fall vor allem deshalb, weil soweit erkennbar zum ersten Mal der Transfer personenbezogener Daten nach China Gegenstand eines Kooperationsverfahrens unter der DS-GVO war und ebenfalls erstmalig Aussagen europäischer Datenschutzaufsichtsbehörden zu den im China bestehenden Datenschutzniveau– jedenfalls bezogen auf ein konkretes Szenario – getroffen wurden.

Der Fall wies einige Besonderheiten auf. Es ging um die Verarbeitung personenbezogener Daten europäischer Nutzer von TikTok im Zeitraum vom 29.07.2020 bis 17.05.2023. Diese Daten wurden auf Servern bestimmter TikTok-Tochtergesellschaften und externer Dienstleister, insbesondere in Singapur und den USA, gespeichert. Eine Speicherung auf Servern in China war nicht Gegenstand des Verfahrens, allerdings hatten Mitarbeiter mehrerer in China ansässiger Unternehmen der TikTok-Gruppe im Rahmen des Supports per Fernzugriff (remote access) von China aus Zugang zu den in den USA und in Singapur gespeicherten Daten. Ein solcher Fernzugriff stellt datenschutzrechtlich eine Übermittlung von Daten aus der EU nach China („Drittlandtransfer") - im Sinne von Kapitel V der DS-GVO- dar, was für sich gesehen auch von TikTok rechtlich nicht in Abrede gestellt worden war. Da für China keine Angemessenheitsentscheidung der Europäischen Kommission im Sinne von Art. 45 DS-GVO bestand bzw. besteht, stützte TikTok diese Übermittlungen auf die Standardvertragsklauseln der Europäischen Kommission (zunächst die Standardvertragsklauseln von 2010, anschließend diejenigen gemäß Durchführungsbeschluss (EU) 2021/914 der Kommission vom 04.06.2021). Wie vom EuGH in seinem Schrems-II-Urteil (EuGH, Urt. v. 16.07.2020, C-311/18) betont, muss ein Datenexporteur bei einem Drittlandtransfer, der auf geeignete Garantien im Sinne von Art. 46 DS-GVO gestützt wird – wie etwa auf die Standardvertragsklauseln der Europäischen Kommission -, die Rechtslage und Praktiken des Drittlands dahingehend überprüfen, ob sich daraus Aspekte ergeben, die es dem Datenimporteur unmöglich machen könnten, seine Verpflichtungen aus dem von ihm eingegangenen Standardvertragsklauseln einzuhalten. Hierfür ist insbesondere zu prüfen, ob die im Drittland bestehenden Zugriffsmöglichkeiten dortiger Behörden auf personenbezogene Daten die im europäischen Recht verankerten Schranken für staatliche Datenzugriffe wahren. Diese den Datenexporteuren abverlangte Prüfung wird mitunter als Transfer Impact Assessment (TIA) bezeichnet.

Zu den Mindeststandards, die das Recht des Drittlands insoweit wahren muss, gehört insbesondere, dass staatliche Zugriffe auf personenbezogene Daten einer verbindlichen gesetzlichen Grundlage bedürfen, die den Umfang und die Voraussetzungen der Datenzugriffe präzise regelt, diese auf das strikt Erforderliche beschränkt und den Grundsatz der Verhältnismäßigkeit wahrt. Ferner müssen für betroffene Personen Rechtsschutzmöglichkeiten vor einem Gericht oder einer vergleichbaren unabhängigen Instanz gegen staatliche Datenzugriffe zur Verfügung stehen.

Auch TikTok stellte nicht in Frage, dass es für die oben geschilderten Übermittlungen personenbezogener Daten nach China ein TIA durchführen musste. Im Rahmen der aufsichtlichen Prüfung legte TikTok hierzu mehrere Rechtsgutachten chinesischer Experten vor. Den Gutachten war letztlich zu entnehmen, dass die Regelungen über Zugriffe chinesischer Sicherheitsbehörden auf personenbezogenen Daten den europäischen Standards von Erforderlichkeit und Verhältnismäßigkeit nicht in vollem Umfang entsprechen (Rn. 301 ff.). Auch belegten die Gutachten, dass die Rechtsschutzmöglichkeiten betroffener Personen gegen staatliche Zugriffe auf personenbezogene Daten den Anforderungen des europäischen Rechts jedenfalls nicht

vollständig genügten (Rn. 326 ff. der Entscheidung). Allerdings vertrat TikTok im Rahmen des Verfahrens die Auffassung, dass die im chinesischen Recht geregelten Zugriffsmöglichkeiten staatlicher Stellen auf personenbezogene Daten nur bei Speicherung von Daten in China zum Tragen kämen, nicht jedoch im vorliegenden Fall, da hier die Daten von China aus nur im Wege des Fernzugriffs abrufbar waren.

Nach Ansicht der federführenden irischen Datenschutzbehörde ließen sich jedoch den von TikTok vorgelegten Gutachten keine hinreichenden Belege für diese von TikTok gezogene rechtliche Schlussfolgerung entnehmen. Zudem betonte die Aufsichtsbehörde, dass selbst bei einem bloßen Fernzugriff auch eine technische Verarbeitung personenbezogener Daten in China - auf den Endgeräten der den Zugriff vornehmenden Personen - erfolge, so dass nicht davon gesprochen werden könne, dass die in Rede stehenden Daten ausschließlich außerhalb des chinesischen Territoriums verarbeitet würden. Die Aufsichtsbehörde betont hierbei, dass sie nicht selbst eine Analyse der maßgeblichen Bestimmungen der chinesischen Rechtsordnung durchgeführt, sondern nur verifiziert hat, ob TikTok selbst nachgewiesen habe, dass für die übermittelten Daten ein mit dem EU-Schutzniveau in der Sache gleichwertiger Schutz gewährleistet ist, was im vorliegenden Fall TikTok nach Ansicht der Aufsichtsbehörde nicht der Fall war.

Dieser von der Aufsichtsbehörde vertretene Ansatz steht im Einklang mit dem „Schrems-II-Urteil" des EuGH, denn der EuGH betont, dass es im Falle eines Drittlandtransfers Aufgabe des Datenexporteurs ist, nachzuweisen, dass er die Rechtsordnung und Praxis des Ziellandes der Übermittlung geprüft hat und dabei zum Ergebnis gekommen ist, dass für die übermittelten Daten ein dem EU-Schutzniveau in der Sache gleichwertiger Schutz gewährleistet ist.

Letztlich hatte TikTok nach Auffassung der Aufsichtsbehörde nicht nachgewiesen, dass die als problematisch – da zu weitgehend – einzustufenden Zugriffsmöglichkeiten chinesischer Behörden auf die in Rede stehenden übermittelten Daten im vorliegenden Fall nicht zum Tragen kommen könnten. Ebendies hätte aber TikTok laut Aufsichtsbehörde nachweisen müssen, da der Datenexporteur nachweisen muss, dass für die übermittelten Daten ein mit dem EU-Datenschutzniveau in der Sache gleichwertiger Schutz gewährleistet ist. Wenn der Datenexporteur diesen Nachweis nicht erbringt bzw. hieran wie im vorliegenden Fall signifikante Zweifel verbleiben, gehen solche Zweifel zu Lasten des Datenexporteurs. Die Aufsichtsbehörde kam somit zum Ergebnis, dass TikTok nicht nachgewiesen hatte, dass die nach China (im Wege der Eröffnung von Fernzugriffsmöglichkeiten) übermittelten personenbezogenen Daten europäischer Nutzer einen mit dem EU-Datenschutzniveau in der Sache gleichwertigen Schutz genießen. Damit stellte die irische Aufsichtsbehörde einen Verstoß von TikTok gegen Art. 46 DS-GVO fest. Die im Kooperationsverfahren beteiligten Aufsichtsbehörden der anderen Mitgliedstaaten haben sich dieser Bewertung angeschlossen, so dass die irische Aufsichtsbehörde wie erläutert am 30.04.2025 eine entsprechende Entscheidung erließ. Die Behörde ordnete die Aussetzung der entsprechenden Übermittlungen personenbezogener Daten nach China an und verpflichtete TikTok, die Verarbeitung in Einklang mit der DS-GVO zu bringen; daneben wurde eine Geldbuße von 485 Mio. Euro verhängt sowie eine weitere Geldbuße in Höhe von 45 Mio. Euro wegen eines im Zusammenhang mit dem Drittlandtransfer stehenden Verstoßes gegen die Pflicht zur Information betroffener Personen.

TikTok hat gegen die Entscheidung Rechtsmittel eingelegt. Der Fall ist aktuell in Irland bei Gericht anhängig. Es bleibt abzuwarten, ob die Gerichte die Position der Aufsichtsbehörden teilen werden. Bemerkenswert ist die Entscheidung in jeden Fall, und zwar nicht nur wegen der verhängten Geldbuße, sondern auch deshalb, weil sie – im Einklang mit der EuGH-Rechtsprechung – die

Nachweispflicht das Datenexporteurs mit Blick auf die Gewährleistung eines mit dem EU-Schutzniveau gleichwertigen Schutzes im Falle eines Drittlandtransfers betont und somit klarstellt, dass verbleibende Zweifel mit Blick etwa auf den Umfang und die Anwendbarkeit staatlicher Zugriffsmöglichkeiten auf personenbezogene Daten im Drittland zu Lasten des Datenexporteurs gehen.

15

Technischer Datenschutz und Informationssicherheit

15 Technischer Datenschutz und Informationssicherheit

15.1 Cyberfestung

Im Rahmen der Cybersicherheitsstrategie 2.0 des Freistaats Bayern veröffentlicht das BayLDA zentrale Maßnahmen zum Schutz vor Cyberattacken für bayrische nicht-öffentliche Stellen.

Die Cybercrime-Szene ist in Bayern nachhaltig aktiv und gefährlich: Täglich erreichen das BayLDA Meldungen bayerischer Firmen über Cyberattacken. Vor diesem Hintergrund hat sich das BayLDA entschieden, noch gezielter über die Gefahren und hilfreiche Präventionsmaßnahmen zu unterrichten. Dabei wird das Bild der „Cyberfestung" als Leitmetapher für die Abwehrstrategie aufgegriffen: Eine Tiefenverteidigung, die darauf abzielt, die Hürden für Angreifer so weit zu erhöhen, dass ein erfolgreicher Angriff unwirtschaftlich oder schlichtweg unwahrscheinlich wird.

Das BayLDA hat sich bei dieser Präventionsarbeit bewusst zur Analogie der uneinnehmbaren Festung entschieden. Historisch betrachtet wurden auch bayrische Burgen durch Kombination mehrerer Verteidigungsanlagen wie Gräben, Mauern und Wachtürme geschützt; die moderne Entsprechung lautet Defense in Depth – die mehrschichtige Verteidigung. Dieses Konzept basiert auf Redundanz: Mehrere, voneinander unabhängige Schutzmechanismen sollen verhindern, dass das Versagen einer einzelnen Komponente das Gesamtsystem kompromittiert. In der Praxis heißt das, technische und organisatorische Maßnahmen so zu kombinieren, dass selbst bei Durchbrüchen auf einer Ebene die nachfolgenden Schichten Angreifer stoppen oder zumindest ihre Wirkung begrenzen.

Für die praxisgerechte Umsetzung wurden vom BayLDA im Jahr 2025 zehn thematische Cyberfestungsbausteine zusammengefasst. Die Bausteine reichen von grundlegenden Konfigurationsprüfungen und Zugangskontrollen bis zur kontinuierlichen Überwachung und Forensikfähigkeiten. Entscheidend ist dabei nicht allein die Existenz einzelner Maßnahmen, sondern ihre Abstimmung und regelmäßige Überprüfung: Ähnlich wie bei einer Burg, bei der auch der Ausfall eines Wachturms durch andere Befestigungsanlagen kompensiert werden muss.

Im Rahmen des Cybersecurity Day 2025 am 29. Januar 2025 präsentierte das BayLDA seinen Ansatz der Cyberfestung erstmalig und stellte die Defense-in-Depth-Methodik vor. Dabei wurden immer wieder die Analogien zu den erfolgreichen Strategien des mittelalterlichen Burgenbaus gezogen. Die Veranstaltung richtete sich an Vertreterinnen und Vertreter aus Politik, Verbänden und Wirtschaft und markierte den Auftakt einer Beratungsoffensive des BayLDA zum Thema „Datensicherheit durch Datenschutz". Parallel zu Veranstaltungen wurde ein konkretes Beratungsangebot etabliert und ausgebaut: Workshops mit Praxisbezug sowie eine 24 Seiten umfassende „Checkliste Cyberfestung – 10 Punkte für mehr Datensicherheit". Diese Angebote waren und sind darauf ausgelegt, unkompliziert und kostenschonend Verbesserungen anzustoßen – gerade weil das BayLDA davon ausgeht, dass bis zu 80 Prozent der Cyberangriffe mit bekannten, einfach umsetzbaren Maßnahmen verhindert werden könnten.

Die Bedrohungslandschaft verändert sich stetig. Der zunehmende Einsatz von Künstlicher Intelligenz gibt Angreifern leistungsfähigere Werkzeuge an die Hand – etwa zur automatisierten Erzeugung täuschend realistischer Phishing-Nachrichten, Angriff-Bots oder zur Auswertung interner Kommunikationsmuster. Zugleich bleibt das Supply-Chain-Risiko zentral: Angriffe über Dienstleister oder Zulieferer können mehrere Organisationen gleichzeitig treffen und die Wirkung eines einzelnen Sicherheitsvor-

falls vervielfachen. Diese Kombination aus technologischer Weiterentwicklung und vernetzten Geschäftsbeziehungen erhöht die Komplexität der Verteidigung erheblich. Die Cyberfestung ist daher weniger als ein starres Konzept zu verstehen als vielmehr ein fortlaufender Prozess – ein Rahmen, der technische, organisatorische und personelle Aspekte verbindet. In Bayern entsteht durch die Bündelung von Sensibilisierung, Checklisten, Beratungsangeboten und regionaler Zusammenarbeit ein pragmatisches Angebot, das insbesondere für kleine und mittlere Unternehmen niedrigschwellige Einstiegsmöglichkeiten bieten soll. Der Ansatz des BayLDA, Prävention weiter auszubauen und leicht umsetzbare Maßnahmen in den Vordergrund zu stellen, reflektiert die Einsicht, dass wirksame Verteidigung oft an der Basis beginnt: Mit sauberen Konfigurationen, Zugangssicherungen und klaren Prozessen.

Gleichzeitig macht die Realität deutlich, dass kein einzelnes Instrument absolute Sicherheit erzeugen kann. Vielmehr ist Resilienz das Ergebnis einer abgestimmten Kombination von Maßnahmen, fortlaufender Überprüfung und situativer Anpassung. Die Metapher der Festung bleibt deshalb hilfreich: Sie verdeutlicht sowohl die Notwendigkeit mehrerer Verteidigungslinien als auch die Bedeutung einer steten Wachsamkeit. Eine Debatte um die Cyberfestung in Bayern ist daher keine rein technische Diskussion, sondern ein integrativer Ansatz zur Erhöhung der Widerstandsfähigkeit von Organisationen. Angesichts der täglichen Meldungen an das BayLDA und der vielfältigen Bedrohungen wirken Prävention, abgestimmte Schutzschichten und institutionelle Unterstützung wie die des BayLDA zusammen. Letztendlich zählt es, die Wahrscheinlichkeit eines erfolgreichen Einbruchs zu senken. In einer vernetzten Wirtschaft bleibt dies eine der zentralen Aufgaben, wenn es darum geht, Geschäftsprozesse, personenbezogene Daten aber auch ökonomische Substanz bayerischer Verantwortlicher zu schützen.

15.2 Ransomware

Die Professionalisierung krimineller Akteure und das systemische Supply Chain Risiko machen Ransomware zu einer gesamtwirtschaftlichen Herausforderung, die über reine IT Sicherheit hinaus auch datenschutzrechtliche Verantwortung erfordert.

Im Jahr 2025 gingen beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) insgesamt 524 Meldungen ein, in denen bayrische Verantwortliche oder deren Dienstleister von Ransomware betroffen waren. Diese Zahl fügt sich in einen über mehrere Jahre in Bayern anhaltenden Trend steigender Meldungen mit Ransomware ein – abgesehen vom Jahr 2024. Aus datenschutzrechtlicher Sicht verlangt diese stetige Entwicklung verstärkte Präventionsmaßnahmen, robuste Reaktionsprozesse und eine engere Koordination zwischen Aufsicht, Strafverfolgung, CERTs und Wirtschaft.

Die Cyberakteure agieren auch im Bereich Ransomware längst arbeitsteilig und marktorientiert: Sogenannte Initial-Access-Anbieter, spezialisierte Ransomware-Operatoren mit vorgefertigten Angriffstools sowie Verhandlungsteams arbeiten zusammen. Technisch zeigt sich der Fortschritt der Täter weniger in neuen, exotischen Exploits als vielmehr in einer stringenten Betriebslogik, die schnelle laterale Bewegungen, gezielten Credential-Diebstahl, Persistenz-Mechanismen und Fernwartungstools kombiniert. Die Angriffsvektoren sind weiterhin erwartbar – Phishing, kompromittierte Fernzugänge, gestohlene Zugangsdaten und Schwachstellen in Drittsoftware – doch gerade ihre Kombination macht sie erfolgreicher und schwerer zu unterbinden.

Für die Wirtschaft in Bayern hatte dies im Jahr 2025 konkrete Folgen. Viele mittelständische Unternehmen, insbesondere aus der Fertigung, dem Maschinenbau und der Zulieferindustrie,

waren aufgrund vernetzter Produktionsanlagen und IT-Verknüpfungen besonders verwundbar. In diesen Betrieben kam es durchaus zu Betriebseinschränkungen wie Produktionsstillstand und Lieferverzögerungen. Datenschutzrechtlich kritisch war der Verlust sensibler Kunden- und Mitarbeiterdaten – in Summe konnten die Schäden durchaus existenzbedrohende Wirkungen entfalten. Zugleich bleiben viele Vorfälle in der Öffentlichkeit weiterhin unsichtbar: Reputationsschutz, laufende Verhandlungen mit Tätern und Versicherungsprozesse führten häufig dazu, dass Vorfälle intern oder nur gegenüber ausgewählten Partnern kommuniziert wurden, sodass die Meldezahlen des BayLDA die tatsächliche Betroffenheit mit hoher Wahrscheinlichkeit nur anteilig abbildet.

Die Datenexfiltration hat sich als zentrales Erpressungsmittel etabliert. Double Extortion, also die Kombination aus Verschlüsselung und der Androhung oder Durchführung der Veröffentlichung gestohlener Daten, ist zur gängigen Praxis geworden. Leak-Seiten, private Foren und direkte Drohungen gegenüber Geschäftspartnern erhöhen den Druck auf Betroffene unabhängig davon, ob interne Systeme technisch schnell wiederhergestellt werden können. Bei Angriffen auf medizinische Einrichtungen – z. B. Arztpraxen und Krankenhäuser – stellt die Veröffentlichung von Patientendaten einen schwerwiegenden, nicht reparablen Schaden der Vertraulichkeit von Gesundheitsdaten dar.

Nicht selten waren Dienstleister initiales Opfer von Ransomware-Attacken: Managed Service Provider und andere IT-Zulieferer fungierten dann als Multiplikatoren, weshalb ein erfolgreicher Einfall zahlreiche Kunden gleichzeitig traf. Dieses Supply-Chain-Risiko macht die Lage für die Wirtschaft auch aktuell schwer überschaubar und wirft konkrete Fragen zu Auftragsverarbeitungsverhältnissen und Sicherheitsanforderungen auf. Die Diskrepanz in der Reaktionsfähigkeit verschärft dabei die Situation: Während Großunternehmen meist über etablierte Incident-Response-Prozesse und bei Bedarf externe forensische Kapazitäten verfügen, agieren viele KMU mit stark begrenzten IT-Ressourcen. Fehlende Logs und unzureichende Backups erschwerten in der Praxis die notwendige Aufklärung und Wiederherstellung, sodass als Folge verlässliche Risikobewertungen und nachhaltige Entscheidungen über eine Benachrichtigungspflicht gegenüber Betroffenen kaum möglich waren.

Aus Sicht der Datenschutzaufsicht ergeben sich daraus klare Handlungsbedarfe. Verantwortliche sollten technische und organisatorische Maßnahmen implementieren, die über Basisschutz hinausgehen: Starke Authentifizierung, Netzwerksegmentierung, regelmäßiges Patchmanagement, getestete Offline-Backups, Mitarbeiter-Schulungen und eine angemessenes Logging waren und sind Voraussetzungen für eine datenschutzkonforme Absicherung – und im Zweifel eben auch für eine forensisch belastbare Reaktion. Das BayLDA setzt daher weiterhin auf präventive Prüfungen, gezielte Beratungen und Informationsangebote für besonders betroffene Branchen sowie die Förderung einer Meldekultur. Die engere Zusammenarbeit mit anderen bayrischen Sicherheitsbehörden im Rahmen der Cyberabwehr Bayern stärkt die Koordination von Reaktionen und die Verteilung von Handlungsempfehlungen. Gleichzeitig sind zielgerichtete Unterstützungsangebote auch künftig notwendig, damit skalierbare Sicherheitsdienste und Förderprogramme breitere Wirkung entfalten.

15.3 E-Mail-Account-Hacking und Phishing

Die fortdauernde Kompromittierung von E-Mail-Accounts führt in Bayern zu signifikanten Datenschutzverletzungen und messbaren wirtschaftlichen Verlusten. Gerade weit verbreitete E- Mail- Dienste stellen hierbei eine besonders exponierte Angriffsoberfläche dar.

Im Jahr 2025 waren kompromittierte E-Mail-Accounts und Phishing-Angriffe weiterhin eine der zentralen Cyberbedrohungen für die Wirtschaft in Bayern. Die Gefährdung war und ist allgegenwärtig, betrifft sowohl große Konzerne als auch den Mittelstand und Freiberufler und entfaltet durch die enge Vernetzung moderner Geschäftsprozesse eine besonders hohe Hebelwirkung.

Weit verbreitete Cloud-Plattformen die verschiedenen Dienste wie E-Mail, Dateiablage und Kollaborationstools kombinieren sind integraler Bestandteil des Arbeitsalltags vieler Unternehmen. Gerade diese weite Verbreitung machen diese aber zu einem attraktiven Ziel für Cyberkriminelle: Das Abgreifen von Zugangsdaten per Phishing hat nicht selten Erfolg. Es werden auch gezielt Phishing-Kits eingesetzt, die auf einen Dienst spezialisiert sind, um Authentifizierungsdaten zu erlangen oder Malware in Systeme einzuschleusen. Aber auch durch Fehlkonfigurationen und ungepatchte Komponenten profitieren Angreifer – eine schlecht konfigurierte Cloud-Instanz oder veraltete Software erleichtert den unerlaubten Zugriff und die rasche Eskalation zu administrativen Rechten. Technisch sind die Verfahren somit in der Masse, d. h. wenn es sich nicht um aufwendig erstellte Spear-Phishing-Attacken oder ähnliches handelt, meist eher unspektakulär: Phishing-E-Mails mit nachgebauten Login-Seiten, Credential-Stuffing aus früheren Leaks oder Brute-Force-Versuche gegen Mailserver genügen häufig, um Konten zu kompromittieren. Interessant ist allerdings die operative Struktur hinter den Angriffen: Automatisierte Masseninstrumente werden mit manueller Aufklärung kombiniert; Access-Broker bieten Initialzugänge zum Kauf an, während spezialisierte Operateure diese Zugänge für Datendiebstahl, Identitätsmissbrauch oder finanzielle Manipulationen nutzen. Dieser Arbeitsteilungseffekt macht Attacken schneller, skalierbarer und in ihrer Wirkung schwerer abzuwehren.

Besonders problematisch ist die Praxis, kompromittierte Konten als Ausgangsbasis für weitere Angriffe zu nutzen. Ein gehackter Account kann zur Versendung täuschend echter Phishing-Mails an Geschäftspartner dienen, zur Manipulation von Zahlungsanweisungen oder zur Exfiltration sensibler Dokumente – und so einen Schneeballeffekt erzeugen, der über Unternehmensgrenzen hinweg wirkt und quasi unaufhaltsam weiter wirkt.

Konkrete Meldedaten aus Bayern unterstreichen das Ausmaß: Im Jahr 2025 gingen beim BayLDA knapp 400 Meldungen von Verantwortlichen ein, die Opfer entsprechender Cyberattacken wurden und eine Meldung nach Art. 33 DS-GVO einreichten. In den betroffenen Fällen waren häufig nicht nur einzelne Konten betroffen. Als Folge des Angriffs wurden in vielen Fällen angegeben, dass zwischen 1.000 und 10.000 weitere E-Mail-Accounts, also auch fremder Organisation, mit der oder einer neuen Angriffstechnik angeschrieben wurden. Dadurch besteht ein hohes Ausbreitungsrisiko. Selbst bei sehr geringer Klickquote kann sich so binnen kurzer Zeit eine rasche Verbreitung einstellen - das infizierte Postfach eines Geschäftspartners wird zum Multiplikator und infiziert Kunden, Zulieferer und weitere Partner – mit unabsehbaren Folgen. E-Mail-Accounts sind in Unternehmen schlichtweg mehr als nur Kommunikationskanäle: Sie enthalten Verhandlungsinhalte, Zahlungsanweisungen, Vertragsentwürfe und sensible personenbezogene Daten. Ein einmal übernommener Account öffnet nicht nur die Tür zu vertraulichen Informationen, sondern bietet auch die Möglichkeit, das Vertrauen in Geschäftsbeziehungen auszunutzen. Manipulierte Zahlungsanweisungen (IBAN-Transaktionsbetrug, CEO Fraud), gefälschte Vertragsdokumente oder Dienstanweisungen aus vermeintlich legitimen Quellen können wirtschaftliche Schäden und Haftungsfragen nach sich ziehen. Darüber hinaus ermöglichen Angreifer langfristige Persistenz – Weiterleitungen, Regelwerke und Archivzugänge werden eingesetzt, um spätere Aktivitäten zu verschleiern.

Die von dieser Welle in Bayern betroffenen Sektoren sind breit gefächert: Der industriell geprägte Mittelstand, Zulieferer im Maschinenbau, IT-Dienstleister und Kanzleien gehören zu den besonders exponierten Gruppen. Unternehmen mit komplexen Zuliefernetzwerken oder hohem Zahlungsverkehr zeigen erhöhte Verwundbarkeit, weil kompromittierte E-Mail-Accounts hier unmittelbar zu Kaskadeneffekten in der Lieferkette führen können. Kleinere Betriebe und freiberufliche Dienstleister sind wegen begrenzter IT-Ressourcen und Zugang zu sensiblen Daten ebenfalls häufig Zielscheibe und Opfer. Allerdings haben sich die Angriffe auf E-Mail-Accounts längst auch auf medizinischen Einrichtungen fortgesetzt: Hier sind die Schäden gerade hinsichtlich der Vertraulichkeit von Gesundheitsangaben besonders gravierend. Mehrere strukturelle Schwächen prägen die aktuelle Lage: Unbedachte Konfigurationen von Cloud-Diensten, fehlendes Login-Monitoring, Verzicht auf Mehrfaktor-Authentifizierung und veraltete Softwareversionen erleichtern Angreifern den Zugang. Organisatorisch erschweren mangelnde Transparenz in Lieferketten, unklare Verantwortlichkeiten und unterschiedliche Sicherheitsstandards bei Dienstleistern die Erkennung und Eindämmung von Vorfällen. Die Folge ist aus Sicht des BayLDA eine hohe Dunkelziffer: Viele Vorfälle werden intern oder innerhalb kleiner Kommunikationskreise behandelt, anstatt bei der zuständigen Datenschutzaufsicht gemeldet zu werden – was die Einschätzung der tatsächlichen Bedrohungslage zusätzlich verkompliziert. Auch scheuen viele Opfer weiterhin davor, eine Strafanzeige bei der Polizei zu stellen.

Die Folgen dieser Sicherheitsproblematik reichen von Datenverlusten und Betriebsunterbrechungen bis zu finanziellen Schäden und langfristigem Vertrauensverlust. Insofern gewinnt die Meldestatistik an Bedeutung: Meldungen nach Art. 33 DS-GVO dokumentieren nicht nur rechtliche Pflichten, sondern zeigen auch die Verbreitungsdynamik solcher Angriffe. Erkennbar wurde so, dass gerade die Angriffe auf E-Mail-Accounts in den vergangenen Jahren in Bayern deutlich zugenommen haben. E-Mail-Account-Hacking und Phishing sind 2025 in Bayern längst keine Randerscheinung mehr, sondern ein systemisches Risiko. Je verbreiteter die Dienste sind, desto eher dienen sie als besonders lukrative Angriffsfläche, so dass bspw. Microsoft365- Umgebungen, aber auch andere große Diensteanbieter wie Gmail oder T-Online in den Fokus rücken. Kompromittierte Accounts wirken oft als Multiplikatoren in Lieferketten und Geschäftsnetzwerken und die wirtschaftlichen wie rechtlichen Konsequenzen können weit über die unmittelbaren IT-Schäden hinausgehen. Es handelt sich um ein flächendeckendes Phänomen, das technische, organisatorische und rechtliche Aspekte zugleich berührt und die Betriebsfähigkeit und das Vertrauen zwischen Geschäftspartnern nachhaltig beeinträchtigen kann. Vor diesem Hintergrund sieht sich das BayLDA bestärkt, seinen präventiven Beratungsansatz im Rahmen der Cybersicherheitsstrategie 2.0 fortzusetzen und so Verantwortliche im nicht-öffentlichen Bereich mit Informationen und Prüfangeboten gezielt zu unterstützen.

16

Bußgeldverfahren

16 Bußgeldverfahren

16.1 Bericht aus der Zentralen Bußgeldstelle

Anzahl der verhängten Geldbußen steigt weiter an.

Ein Großteil der von der Zentralen Bußgeldstelle im Berichtszeitraum bearbeiteten Fälle ging weiterhin auf Ordnungswidrigkeitenanzeigen der Polizei zurück. Allerdings war auch eine weitere Steigerung von Abgaben aus den Fachbereichen festzustellen. Auffallend war eine Häufung von Fallabgaben, in denen Verantwortliche im Verwaltungsverfahren ergangener Anweisungen – trotz zum Teil mehrerer angedrohter Zwangsgelder - nicht nachgekommen sind. In diesen Fällen wurden konsequent Bußgeldverfahren eingeleitet und in einem Fall bereits mit Geldbuße sanktioniert (siehe dazu Kapitel 4).

Im Berichtszeitraum wurden Bußgelder gegen Unternehmen und Privatpersonen in einer insgesamt hohen fünfstelligen Höhe verhängt, wobei nicht alle Entscheidungen bis zum Redaktionsschluss rechtskräftig wurden. Die Spanne der festgesetzten Geldbußen reicht von einer Sanktion gegen eine Privatperson in zweistelliger Höhe bis zu einer Geldbuße gegen ein Unternehmen im mittleren fünfstelligen Bereich. Weitere im Berichtsjahr geführte Verfahren in sechsstelliger Größenordnung standen unmittelbar vor Redaktionsschluss kurz vor dem Abschluss. Geahndet wurden im Wesentlichen unrechtmäßige Verarbeitungen und Verstöße gegen Transparenzvorschriften.

Wie im Vorjahr betrafen viele Vorgänge den Einsatz von Videoüberwachung und GPS- bzw. Bluetooth-Tracking durch Privatpersonen und Unternehmen sowie die Veröffentlichung im Internet. Daneben wurde erneut ein öffentlicher „Fahndungsaufruf" durch den Betreiber eines „24/7-Automaten-Shops" sanktioniert. Dieser erhoffte sich durch die Veröffentlichung von Bildern aus der Videoüberwachung Hinweise zur Identifizierung von zwei Personen, die er des Diebstahls und der Sachbeschädigung verdächtigte.

Daneben ahndete das Bayerische Landesamt für Datenschutzaufsicht, wie bereits auch in den Vorjahren, die allgemein zugängliche Veröffentlichung sensibler personenbezogener Daten, wie der Telefonnummer oder der Adressdaten, im Internet mit Geldbuße, wenn hierfür kein Rechtfertigungsgrund bestand. Beispielhaft kann hier ein Fall vorgehoben werden, in dem ein Pfleger in einer Senioreneinrichtung während seines Dienstes aus dem Stationszimmer einen Livestream auf dem Videoportal TikTok veröffentlichte, in dem er Namen von Bewohnern und Kollegen erwähnte.

Erwähnenswert sind zudem zwei Einzelfälle, in denen mit Ortungsgeräten der Aufenthaltsort anderer Personen in Erfahrung gebracht werden sollte:

In einem Fall wurde in einem Firmenfahrzeug, welches einem Mitarbeiter zur Durchführung von beruflich veranlassten Fahrten zur Verfügung gestellt wurde, zwei Mal versteckt ein Apple-AirTag angebracht. Zunächst wurde ein solches ohne Information des Beschäftigten in eine sich im Fahrzeug befindliche Fahrzeugmappe gelegt. Nachdem dieser durch Mitteilungen auf sein Handy auf das AirTag aufmerksam gemacht worden war und es entfernt und der Polizei übergeben hatte, wurde erneut ein Apple-AirTag, diesmal unter dem Polster des Fahrersitzes versteckt, angebracht. Auch auf dieses wurde der Mitarbeiter durch Benachrichtigungen auf sein Handy aufmerksam. Der Mitarbeiter übergab dieses AirTag ebenfalls der zuständigen Polizeiinspektion. Durch weitere Ermittlungen konnte die Einzelunternehmerin als Verantwortliche identifiziert werden. Diese trug

vor, die AirTags aus steuerlichen Gründen, nämlich zur Überwachung der ausschließlich beruflichen Nutzung des Pkws durch ihren Mitarbeiter, sowie zur Vermeidung von Diebstahl, angebracht zu haben. Da ein heimliches Tracking mittels Apple-AirTag weder tauglich noch erforderlich war, um gegenüber den Finanzbehörden eine ausschließlich beruflich veranlasste Nutzung des Firmenfahrzeugs nachzuweisen oder einen Diebstahl des Fahrzeuges zu verhindern, wurde der Einsatz mit Geldbuße sanktioniert. Aufgrund der wirtschaftlichen Situation der Einzelunternehmerin wurde eine Geldbuße im oberen vierstelligen Bereich verhängt. Allgemeine Informationen zur Zulässigkeit von GPS- bzw. Bluetooth-Tracking im Beschäftigtenverhältnis befinden sich in Kapitel 9.

In einem anderen Fall wurde ein GPS-Tracker durch einen Sicherheitsdienst eingesetzt. Das Unternehmen wurde von einer Frau zum Personenschutz beauftragt, weil sie sich von ihrem Ex-Partner bedroht, verfolgt und belästigt fühlte. Der Ex-Partner der Frau wurde von Mitarbeitern des Sicherheitsdienstes zunächst einige Tage beobachtet. Der Verdacht, dass sich dieser häufig in räumlicher Nähe zu der Auftraggeberin aufhielt, bestätigte sich dabei zwar, allerdings konnte nicht festgestellt werden, dass von diesem konkrete Gefahren für die Dame ausgingen. Dennoch wurde durch das Sicherheitsunternehmen an dem Fahrzeug des Ex-Partners schließlich ein GPS-Tracker angebracht. Da die Anbringung des Ortungsgerätes aus Sicht des Bayerischen Landesamtes für Datenschutzaufsicht nicht erforderlich war, wurde auch dieser Einsatz mit einer Geldbuße im mittleren vierstelligen Bereich sanktioniert, wobei die wirtschaftliche Situation des Sicherheitsunternehmens die Höhe der Geldbuße maßgeblich beeinflusste. Zum Schutz der Frau standen nach Auffassung des Bayerischen Landesamtes für Datenschutzaufsicht mildere Mittel zur Verfügung, wie die weitere Beschattung des Ex-Partners oder die Begleitung der Auftraggeberin. Daneben konnte bei der Observation auch keine konkrete Gefahrensituation für die Auftraggeberin festgestellt werden.

Der Arbeitskreis Sanktionen der DSK, der von dieser im Berichtszeitraum in „Arbeitskreis Rechtsdurchsetzung" umbenannt wurde, finalisierte im Jahr 2025 zwei Handreichungen für die Bußgeldstellen der Datenschutzaufsichtsbehörden (Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden und Merkblatt zur Verständigung), die den Arbeitskreis bereits seit Längerem beschäftigten.

Die Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden stellen eine Praxishandreichung dar, die die Verfahren der Datenschutzaufsichtsbehörden weitgehend harmonisieren sollen. Nach dem entsprechenden Beschluss der DSK sollen diese von den Aufsichtsbehörden der Länder und des Bundes (soweit diese für den nicht-öffentlichen Bereich zuständig sind) für den jeweiligen Zuständigkeitsbereich als Verwaltungsvorschriften in Kraft gesetzt werden. Die Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden sind auf der Homepage der DSK veröffentlicht (DSK-Festlegung MRiDaVG.pdf).

Ebenfalls finalisiert werden konnten von dem AK Rechtsdurchsetzung im Jahr 2025 die Arbeiten an einem Merkblatt zur Verständigung, das die Rahmenbedingungen für die Beendigung eines datenschutzrechtlichen Verfahrens über Geldbußen durch eine einvernehmliche Verständigung beschreibt und ebenfalls auf der Homepage der Datenschutzkonferenz veröffentlicht ist (DSK Merkblatt Verstaendigung.pdf).

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 hervorzuheben.

Stichwortverzeichnis

A

Angemessenheitsbeschluss 64
Anweisung 22
Arztpraxis 50
Auskunft 57, 58
Auskunftei 28

B

Beratungen 13
berechtigten Interesses 56
Beschäftigtendatenschutz 40
Bescheid 23
Beschwerden 10
Betroffenenrechte 51
Bluetooth-Tracking 76
Bonität 28
Bußgeldverfahren 76

C

China 65
Cyberfestung 70
Cybersicherheit 70

D

Dashcam 47
DataAct 60
Datenschutzbeauftragte 25
Datenschutzverletzungen 14
Datenweitergabe 60
Digitalwirtschaft 56
Drittlandübermittlung 64, 65

E

Einwilligung 51
E-Mail-Account 72
E-Mail-Kommunikation 53
E-Mail-Postfach 41
Europäische Zusammenarbeit 16
EU-US-Data Privacy Framework 64

F

Finanzwirtschaft 27
Firmenfahrzeug 42

G

Geldbuße 21, 76
Geldforderung 27
Geschäftsführer 40
Gesundheit 50
gleichwertiger Schutz 67

H

Hacking 73
Handelsregister 40
Hausordnung 36

I

Identität 34
Identitätsdiebstahl 59
Informationssicherheit 70
Inkasso 27, 28
Internationaler Datenverkehr 64
Internet 56, 76

K

Klimamonitoring 37
Kooperationspflicht 22
Kooperationsverfahren 16
Kopie 57
Kreditinstitut 28
Kündigung 40

L

Löschung 21, 28

M

Microsoft Outlook 21

N

Nachweispflicht 68

O

Offboarding 42
Online-Account 57
Onlinehandel 58
Ortungsgerät 76

AirTag 76
GPS-Tracker 42, 77

P

Personalausweis
Kopie 34
Pfand 35
Phishing 73
politische Werbung 61
Profilingverfahren 62

R

Ransomware 71
Rauchwarnmelder 37
Rechtsanwälte 53

S

Smart-Home-Geräten 60
Statistik 10
Subgroups 18
Supply-Chain-Risiko 72

T

Targeting 61
Technischer Datenschutz 70
Telemedien 56
Terminbuchung 50
Terminmanagement 50
Transfer Impact Assessment 66
Transkription 56
Transparenz 61

V

Verfahrensverordnung 16
Veröffentlichung 76
Versicherungen 50
Vertraulichkeit 25
Videokonferenzen 56
Videoüberwachung 47, 76

W

Werbung 31
Widerruf 51
Wohnungseigentümergemeinschaft 36
Wohnungswirtschaft 34

Z

Zahlen und Fakten 10
Zentrale Bußgeldstelle 76
Zwangsgeld 22

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