Landtag von Baden-Württemberg **Drucksache 17 / 10322**

17. Wahlperiode **23.3.2026**

Mitteilung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

41. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg für das Jahr 2025

Schreiben des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 23. März 2026:

Anbei übersende ich Ihnen meinen 41. Tätigkeitsbericht Datenschutz für das Jahr 2025.

Prof. Dr. Keber

Eingegangen: 23.3.2026 / Ausgegeben: 30.3.2026

Menschen schützen – Technik gestalten

41. Tätigkeitsbericht Datenschutz 2025

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Menschen schützen – Technik gestalten

41. Datenschutz-Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz und
die Informationsfreiheit Baden-Württemberg 2025

Baden-Württemberg

Inhalt

Vorwort

Prof. Dr. Tobias Keber

Das vergangene Jahr 2025 war geprägt von einer sich rasant weiterentwickelnden Datenschutzlandschaft: Die Digitalisierung beinahe aller Lebensbereiche, die zunehmende Bedeutung von künstlicher Intelligenz und die wachsende Abhängigkeit von digitalen Technologien stellen unsere Gesellschaft und Wirtschaft vor große Herausforderungen. Auch das Aufgabenportfolio des Landesbeauftragten wird durch neue europäische Digital- und Datenrechtsakte zunehmend komplexer.

Die Bedeutung von datenschutzkonform gestalteten Technologien unterstreicht der signifikante Anstieg der Beschwerdezahlen von über 90 % innerhalb eines Jahres, der nicht nur in der hiesigen Aufsichtsbehörde zu verzeichnen ist. Es zeigt sich: Der verantwortungsvolle und sichere Umgang mit ihren persönlichen Daten ist den Menschen wichtig. Wer nachhaltigen technischen Forstschritt will, braucht das Vertrauen der Menschen. Vertrauen wird nur geschaffen, wenn technische Entwicklung menschenzentriert erfolgt.

So erklärt sich auch der Titel des 41. Tätigkeitsberichts: Menschen schützen – Technik gestalten. Das klingt selbstverständlich, ist aber nicht trivial. Es geht um Orientierung und Prioritäten. Der Mensch steht im Mittelpunkt, Technik, Innovation und das Recht sind gestaltbar, müssen aber stets an den Bedürfnissen der Menschen ausgerichet werden. Gestaltung geht nur gemeinsam. Interdisziplinär, unterschiedliche Perspektiven einbeziehend. Das macht unser Titelbild auf Vorder- und Rückseite deutlich: Auf der Vorderseite der Mensch. In der technisierten Welt hinterlässt er zwangsläufig digitale Spuren. Wie durchsichtig der Vorhang ist, entscheidet die Gesellschaft. Das tut sie auf Grundlage von Diskurs, der in Form gebracht und umgesetzt werden muss. Visualisiert haben wir dies auf der Rückseite unseres Tätigkeitsberichts.

Die stark steigenden Beschwerdezahlen und die zunehmende Aufgabenkomplexität füllen unsere Kapazitäten voll aus. Der Wegfall der Stellen für das Projekt „Datenschutz geht zur Schule“ im vergangenen Jahr hat unsere strukturellen Beratungstätigkeiten belastet. Durch das Bildungszentrum Datenschutz und Informationsfreiheit (BIDIB) ist es aber weiter gelungen, Schulungen zu ganz unterschiedlichen Themen anzubieten und viele Behörden, Unternehmen und Bürger_innen zu erreichen. Zudem gehen wir ver-

mehrt auf die Verantwortlichen zu, sprechen auf Messen und Kongressen mit ihnen, organisieren themenspezifische Veranstaltungen und laden zum Austausch ein.

Wir waren im letzten Jahr in zahlreichen Gesetzgebungsverfahren beratend beteiligt und haben landespolitische Debatten konstruktiv begleitet. Für die vertrauensvolle und stets konstruktive Zusammenarbeit danke ich dem Landtag von Baden-Württemberg und den Mitgliedern der Landesregierung sehr herzlich.

Besonders geprägt war das vergangene Jahr organisatorisch auch durch den Umzug der Behörde in neue Räumlichkeiten zum Jahreswechsel 2025/2026.

Das kommende Jahr 2026 wird im Zeichen des baden-württembergischen Vorsitzes der Datenschutzkonferenz des Bundes und der Länder (DSK) stehen und damit sowohl mit der Chance verbunden sein, gestaltend zu wirken, als auch dem Auftrag verpflichtet sein, die Bedeutung des Datenschutzes nicht nur landesweit, sondern in enger Abstimmung der Bundes- und Landesdatenschutzaufsichtsbehörden, auch in Richtung Europa gemeinschaftlich zu stärken.

Der 41. Tätigkeitsbericht orientiert sich an der Struktur des vergangenen Berichts und ordnet die Beiträge den aufsichtsrechtlichen Aufgabenbereichen der DS-GVO zu. Gegliedert ist der Bericht in zwei größere Abschnitte, einen ersten Abschnitt mit abteilungsübergreifenden Schwerpunkten und den großen Entwicklungslinien im Daten- und Digitalrecht sowie einen zweiten Abschnitt mit Berichten aus den Fachabteilungen.

Ihr Landesbeauftragter

Prof. Dr. Tobias Keber

DSK
DATENSCHUTZKONFERENZ
Baden-Württemberg 26

Die Datenschutzkonferenz (DSK) ist der Zusammenschluss der staatlichen Datenschutzaufsichtsbehörden Deutschlands und besteht aus den Datenschutzbeauftragten des Bundes und der 16 deutschen Bundesländer. Sie hat zum Ziel, die Aktivitäten zwischen den Aufsichtsbehörden abzustimmen und gemeinsame Positionen festzulegen, mit denen das europäische und nationale Datenschutzrecht deutschlandweit einheitlich umgesetzt und weiterentwickelt werden kann.

Im Jahr 2026 hat Baden-Württemberg den Vorsitz der DSK.

Kapitel 1

Vom Schreibtisch des LfDI

1. Vom Schreibtisch des LfDI

Die datenpolitische Großwetterlage im Jahr 2025 war ebenso stark in Bewegung, wie auf europäischer, Bundes- und Landesebene vielfältige Entwicklungen mit Relevanz für den Datenschutz zu beobachten waren.

Daten- und Digitalrecht: das Jahr 2025 im Rückblick

In Baden-Württemberg haben wir auch in diesem Jahr wieder einen starken Fokus auf Beratung im Kontext von KI gesetzt. So haben wir zahlreiche Projekte in den Bereichen Bildung und Gesundheit eng begleitet und die verantwortlichen Stellen beraten. Insbesondere herauszuheben ist das Projekt MEDI:CUS zur Entwicklung einer cloudbasierten Medizindaten-Infrastruktur. Diese bereits etablierte, vertrauensvolle Zusammenarbeit mit öffentlichen Stellen der Länder sowie an den Projekten beteiligten Unternehmen werden wir auch künftig fortsetzen. Der Beratungsbedarf ist hoch.

Im Januar 2025 machte die Entlassung dreier demokratischer Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB) in den USA Schlagzeilen. Das PCLOB ist wichtiges Element des EU-US Data Privacy Framework (DPF/TADPF), das den transatlantischen Datentransfer legitimiert. Das Europäische Parlament stellte hierauf eine formelle Anfrage an die Kommission, ob der Angemessenheitsbeschluss angesichts dieser Entwicklung noch tragfähig sei. Vor diesem Hintergrund steht dann das unten (s. Kap. 5.5.10.) eingehend dargestellte erstinstanzliche Urteil des EuG vom 3. September 2025. Im Ergebnis wies das EuG die Nichtigkeitsklage des französischen Abgeordneten Latombe ab. Dieser legte am 31. Oktober 2025 Berufung beim Europäischen Gerichtshof (EuGH) ein, wo das Verfahren unter dem Aktenzeichen C-703/25 P noch anhängig ist.

Seit dem 2. Februar 2025 dürfen nach dem gestuften Zeitplan der KI-Verordnung (KI-VO) die dort als verboten klassifizierten Praktiken (Art. 5) nicht mehr angewandt werden. Weiter gelten die Regeln zur KI-Kompetenz (Art. 4), wonach Anbieter und Betreiber von KI-Systemen verpflichtet sind, Maßnahmen zu ergreifen, damit ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen betraut sind, über hinreichende KI-Kenntnisse verfügen. Im Jahr 2026 werden nach Art. 57 KI-VO KI-Reallabore einzurichten sein, was für Forschende, Unternehmen, aber auch die beteiligten Aufsichtsbehörden große Chancen bedeutet. Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) hat am 12. September 2025 einen Referentenentwurf für ein Gesetz zur Durchführung der KI-Verordnung vorgelegt, den die Datenschutzkonferenz im Oktober ausführlich kommentiert und auf Defizite hin-

Infokasten

Anfrage des Parlaments: Suspension of US Privacy and Civil Liberties Oversight Board investigations and its impact on EU-US data transfers: https://www.europarl.europa.eu/doceo/document/P-10-2025-000941_EN.html

Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, vom 10. Oktober 2025: https://www.datenschutzkonferenz-online.de/media/st/Stellungnahme_Durchfuehrungsgesetz_KI-VO.pdf

gewiesen hat. Zu Redaktionsschluss dieses Tätigkeitsberichts läuft das Gesetzgebungsverfahren noch.

Am 11. Februar 2025 zog die EU-Kommission den Entwurf der ePrivacy-Verordnung offiziell zurück – nach acht Jahren erfolgloser Verhandlungen. Die Verordnung sollte die DS-GVO im Bereich elektronische Kommunikation ergänzen (Cookies, Metadaten, Tracking – dazu unten Kap. 5.). Die Kommission begründete den Rückzug mit fehlender Einigung der Ko-Gesetzgeber und (teilweiser) Überholung durch neuere Verordnungen (Digital Markets Act – DMA, Digital Services Act – DSA). Praktische Folge ist, dass die ePrivacy-Richtlinie von 2002 weiterhin gilt.

Am 5. März 2025 wurde die Verordnung (EU) 2025/327 zum European Health Data Space (EHDS) im Amtsblatt der EU veröffentlicht, sie trat am 26. März 2025 in Kraft. Die Anwendbarkeit der Regelungen erfolgt stufenweise, erste allgemeine Regeln zum 26. März 2027, zentraler Stichtag für die wesentlichen Teile der Verordnung ist dann der 26. März 2029. Der EHDS schafft einen EU-weiten Rechtsrahmen für den Zugang zu elektronischen Gesundheitsdaten – sowohl für die Patientenversorgung (Primärnutzung) als auch für Forschung, Innovation und Politikgestaltung (Sekundärnutzung). Die Verordnung spielt in unserer Beratung (vgl. hierzu Kap. 3.5. und 3.6.) bereits eine wichtige Rolle, wo sie gesundheitsdatenschutzrechtliche Regelungen im Bundes- (GDNG) und Landesrecht (LKHG) künftig formen wird.

Am 9. April 2025 stellten CDU/CSU und SPD den Koalitionsvertrag „Verantwortung für Deutschland“ vor, der auch datenschutzpolitische Vorhaben enthält. Wie weit diese unions- und verfassungsrechtlich realisierbar sind, wird sich zeigen. Die Datenschutzaufsichtsbehörden der Länder hatten schon zuvor einstimmig Eckpunkte für eine freiheitliche und grundrechtsorientierte digitale Zukunft und dafür erforderliche Strukturmaßnahmen vorgeschlagen. Es ist möglich, bürokratiearme und zugleich grundrechtswahrende Strukturen zu schaffen. Wie dies in der Praxis gelingen kann, zeigen wir unten an einem konkreten Beispiel (s. Kap. 5.3.1.).

Am 2. Mai 2025 verhängte die irische DPC ein Bußgeld in Höhe von 530 Millionen Euro gegen TikTok für rechtswidrige Datenübermittlungen nach China und Verstößen gegen den Transparenzgrundsatz. Das Unternehmen hat am 27. Mai 2025 Rechtsmittel beim Irish High Court eingelegt, das Verfahren läuft noch.

Den datenschutzrechtlichen Diskurs im Mai 2025 bestimmte auch Metas Plan, europäische Nutzendendaten von Facebook und Instagram für KI-Training zu verwenden. Die Verbraucherzentrale NRW forderte den

Infokasten

Text der Verordnung des European Health Data Space (EHDS): Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847: https://eur-lex.europa.eu/eli/reg/2025/327/oj/eng

#AgendaGesundheit Forum, Gesundheitsdaten intelligent nutzen – Potenzial für innovative Versorgung, Medizin und Forschung, Diskussion vom 19. November 2025: https://www.aok.de/pp/bw/nachricht/aufzeichnung-19112025/

Verantwortung für Deutschland. Koalitionsvertrag zwischen CDU, CSU und SPD, 21. Legislaturperiode: https://www.koalitionsvertrag2025.de/

Bewertung: LfDI über die Ergebnisse der Koalitionsverhandlungen in Berlin: https://www.baden-wuerttemberg.datenschutz.de/lfdi-ueber-die-ergebnisse-der-koalitionsverhandlungen-in-berlin/

DSK-Entschließung „Eckpunkte für eine freiheitliche und grundrechtsorientierte Digitale Zukunft", vom 26. März 2025: https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Datenschutzpolitisches_Eckpunktepapier.pdf

Irish Data Protection Commission (DPC) fines TikTok €530 million and orders corrective measures following Inquiry into transfers of EEA User Data to China: https://www.data-protection.ie/en/news-media/latest-news/irish-data-protection-commission-fines-tik-tok-eu530-million-and-orders-corrective-measures-following

LfDI Tobias Keber diskutierte beim „#AgendaGesundheit Forum“ über intelligente Gesundheitsdatennutzung und wie Versorgung, Medizin und Forschung datenschutzfreundlich umgesetzt werden kann. Auf dem Bild: Johannes Bauernfeind (Vorstandsvorsitzender der AOK BW), Christoph Schickhardt (Institut für Medizin- und Datenethik, Medizinische Fakultät, Universität und DKFZ Heidelberg), Melanie Börries (Leiterin des Instituts für Medizinische Bioinformatik und Systemmedizin am Universitätsklinikum Freiburg), LfDI Tobias Keber, Nicole Krieger (Moderatorin), Peer-Michael Dick, Alternierender Vorsitzender des Verwaltungsrates der AOK BW (v.l.n.r.:). Bild: AOK Baden-Württemberg

Konzern auf, den für den 27. Mai 2025 geplanten Rollout zu stoppen. Meta berief sich für die Rechtmäßigkeit der Datenverarbeitung auf berechtigte Interessen im Sinne des Art. 6 Abs.1 Buchst. f) DS-GVO und bot nur eine Opt-out-Möglichkeit statt einer aktiven Einwilligung an. Das OLG Köln wies den Antrag der Verbraucherzentrale ab. In der Begründung des Gerichts spielten unser Diskussionspapier „Rechtsgrundlagen beim Datenschutz beim Einsatz von KI“, die Stellungnahme des EDSA (s. Infokasten) und die Rechtsprechung des EuGH zum Suchmaschinenprivileg eine wichtige Rolle. Insgesamt offenbarte das Verfahren, dass Anpassungen des europäischen Daten- und Digitalrechts mit Blick auf Künstliche Intelligenz und Plattformregulierung dringend diskutiert werden müssen.

Im Juni 2025 hat die DSK die „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen“ veröffentlicht. Sie richtet sich vorrangig an Hersteller_innen und Entwickler_innen von KI-Systemen und soll ihnen als Hilfestellung bei der datenschutzkonformen Entwicklung von KI-Systemen dienen. Dabei soll sie auch dabei helfen, die technischen

Infokasten

DSK-Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen: https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf

Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA): https://www.baden-wuerttemberg.datenschutz.de/onkida/ ;Video: ONKIDA–Orientierungshilfen-Navigator KI & Datenschutz: https://tube.bawü.social/w/m9vWviMyhzWyeLCBGnEgP1

Stellungnahme des EDSA zu KI-Modellen: DSGVO-Prinzipien unterstützen verantwortungsvolle KI vom 18. Dezember 2024: https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_de

Entwicklungsmöglichkeiten im Beschaffungsprozess zu berücksichtigen. Die neue Orientierungshilfe zeigt, wie Datenschutz von Anfang an berücksichtigt werden kann („Data Protection by Design“) und somit die Rechte und Freiheiten natürlicher Personen geschützt werden können.

Am 17. Juli 2025 entschied das VG Köln (13 K 1419/23) in einem Verfahren, in dem es um den Betrieb der Facebook-Fanpage des Bundespresseamts (BPA) ging. Das BPA hatte gegen einen Bescheid der Bundesdatenschutzbeauftragten aus dem Februar 2023 geklagt, in dem der Betrieb der Facebook-Fanpage wegen Datenschutzmängeln untersagt worden war. Das Gericht verneinte eine gemeinsame Verantwortlichkeit von Bundespresseamt und Meta nach Art. 26 DS-GVO. Das Urteil steht allerdings in deutlicher Spannung zur EuGH-Rechtsprechung, weshalb der Ausgang des Berufungsverfahrens vor dem OVG Münster mit großem Interesse zu erwarten ist.

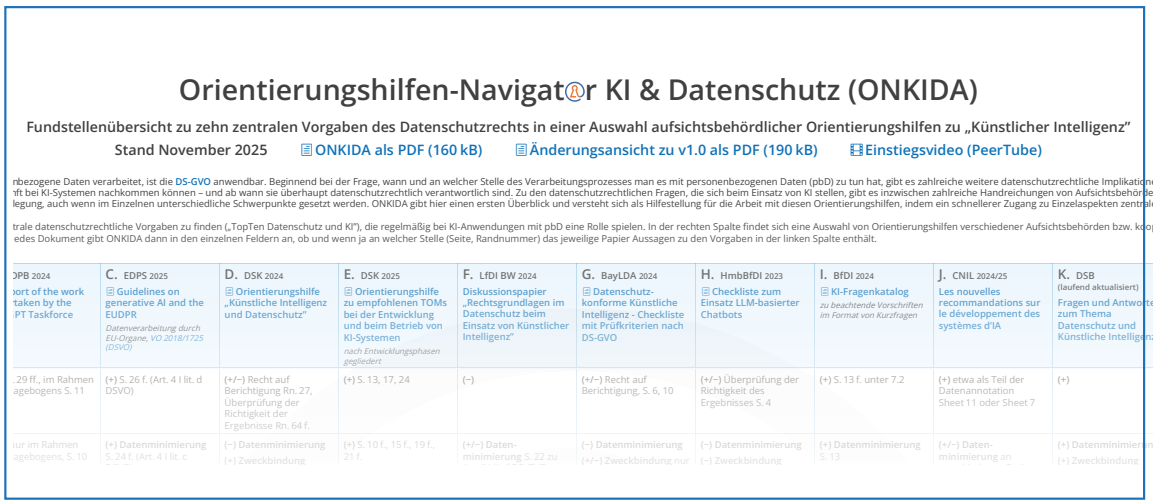
Seit dem 12. September 2025 sind die zentralen Pflichten des EU Data Act anwendbar. Die Verordnung schafft neue Rechte auf Datenzugang bei vernetzten Produkten, verpflichtet Cloud-Anbieter zu Wechselmöglichkeiten und soll Lock-in-Effekte reduzieren. Handelt es sich bei den zu übermittelten Daten um personenbezogene, sieht das Europarecht die Datenschutzbehörden als Aufsicht für die Einhaltung der Bestimmungen des Data Acts vor (Art. 37 Abs. 3 Data Act). Die nähere Ausgestaltung der Zuständigkeiten auf nationaler Ebene im Rahmen eines Durchführungsgesetzes ist noch nicht abgeschlossen.

Im Oktober 2025 wurde die „Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode“ veröffentlicht (s. Kap 2.4.).

Infokasten

Urteil im Fall Fanpages liegt vor: BfDI prüft weitere rechtliche Schritte: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2025/11_Urteil-Fanpages.html

Data Act: Gesetzentwurf zur Durchführung vorgelegt: https://www.bundestag.de/presse/hib/kurzmeldungen-1128820



Eine Übersicht, die in der Praxis hilft: Wer Datenschutz und KI zusammenbringen will, kann die vom LfDI zur Verfügung gestellte Übersicht nutzen. Damit der Einstieg besonders leicht fällt, hat der LfDI auch ein einordnendes Video erstellt. Die Übersicht wird kontinuierlich weiterentwickelt und um neue Informationen ergänzt.

Mit der Änderung des Polizeigesetzes vom 18. November 2025 hat der Landesgesetzgeber für die Polizei Baden-Württemberg die Erlaubnis zur verfahrensübergreifenden Recherche und Analyse geschaffen. Die verfassungs- und datenschutzrechtlichen Vorgaben für ein derart grundrechtssensibles Projekt sind hoch, worauf ich in meiner Stellungnahme im Gesetzgebungsverfahren sowie im Petitionsausschuss hingewiesen habe. Details hierzu finden Sie in Kap. 3.2.

Am 19. November 2025 präsentierte die EU-Kommission das „Digital Omnibus Package" – ein umfassender Reformvorschlag, der unter anderem die DS-GVO, die ePrivacy-Richtlinie, den Data Act und die KI-VO ändern soll. Ziel soll die Vereinfachung und Entbürokratisierung des Rechts sein. Ob das mit den Vorschlägen in ihrer bisherigen Form tatsächlich gelingen kann, wird sich zeigen. Im Rahmen der Trilog-Verhandlungen zwischen Kommission, Rat und Europäischem Parlament wird es vermutlich noch zahlreiche Änderungen geben.

Am 12. Dezember 2025 hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder Reformvorschläge für die Datenschutz-Grundverordnung vorgelegt und den Bedarf für Rechtsgrundlagen bezüglich der Entwicklung und des Betriebs von KI-Modellen und -Systemen unterstrichen. Zugleich wurde betont, dass zur Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen und -Systemen auch gehört, Transparenzvorgaben und Betroffenenrechte der DS-GVO zu gewährleisten. In der Reform des Landesdatenschutzgesetzes (zum Redaktionsschluss lag noch keine Entschiedung des Parlamentes vor), bei der wir ebenfalls beratend tätig waren, spielten Rechtsgrundlagen für KI eine wesentliche Rolle.

Infokasten

Digital-Omnibus-Verordnung: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837

LfDI Tobias Keber diskutierte auf der KI-Woche 2025 mit Martin Andree, Wolfgang Kreißig und Peter Nägele (v.l.n.r.) über digitale Souveränität, Plattformregulierung und wie mit KI-Reallaboren Künstliche Intelligenz made in BW gefördert werden kann. Bild: LfDI BW

Die steigende Bedeutung von KI-Reallaboren zur Errichtung von geschützten, regulatorischen Lernräumen zeigt, dass wir auch hier auf dem richtigen Weg sind. Im kommenden Jahr werden wir daher unsere Beratungsleistung im Bereich KI weiter intensivieren, Reallabore begleiten und uns in interdisziplinären Netzwerken dafür einsetzen, auch KI-Reallabore begleiten zu können.

Entwicklung unserer Dienststelle

In diesem Jahr haben wir beinahe eine Verdopplung der Beschwerdezahlen zu verzeichnen (von 4034 im Jahr 2024 auf 7673 im Jahr 2025), die Zahl der Datenpannenmeldungen stieg um knapp 20 Prozent. Unsere Kolleg_innen im Haus arbeiten mit Hochdruck daran, bestmöglich und wirksam Bürger_innen, Behörden und Unternehmen zu helfen und das moderne Grundrecht Datenschutz zu stärken. Ihnen danke ich für ihren herausragenden Einsatz.

Auch in diesem Jahr haben wir wieder intensiv die Landesregierung beraten im Gesetzgebungsprozess, waren im Austausch mit Städten und Gemeinden. Wir haben Unternehmen beraten und Handreichungen und Orientierungshilfen herausgegeben. Viele Bürgerinnen und Bürger haben wir mit bewährten und neuen Schulungs- und Veranstaltungsformaten angesprochen. Für uns als Aufsichtsbehörde ist es wichtig, dass wir unser Wissen einer breiten Öffentlichkeit vermitteln. Zugleich ist für uns als lernende Behörde elementar, neues Wissen in unser Haus holen.

Wir werden unseren konsequenten Beratungsansatz auch künftig fortsetzen, dabei weiter interdisziplinär arbeiten. Nur so können wir die Wissenschaftler_innen aus unseren exzellenten Hochschulen und Forschungseinrichtungen, die großen und kleinen innovativen Unternehmen sowie die interessierte Bürgerschaft beraten.

Im vergangenen Jahr mussten wir wie andere Dienststellen auch mit weniger Ressourcen auskommen. Im Personalbereich verfügte unsere Dienststelle im Jahr 2024 über 70,5 Personalstellen, seit dem Jahr 2025 sind es nur noch 67,5 Personalstellen. Der Landtag hatte uns dankenswerter Weise drei befristete Stellen für den Schulbereich bestätigt, die uns halfen, unser Beratungsangebot „Schule Digital“ in unserem Bildungszentrum zu forcieren. Auf diese Stellen konnten wir im vergangenen Jahr nicht mehr zurückgreifen. Wir haben versucht weiterhin gute Beratungsangebote vorzuhalten, unsere Kolleg_innen im Haus haben den Personalverlust bestmöglich aufgefangen. Gleichwohl war es nicht möglich, die Schulen wie die Jahre zuvor zu unterstützen, was wir sehr bedauern, ist der Bedarf nach unserer Erfahrung doch eher gestiegen als gefallen, insbesondere wenn man auf den Einsatz von KI in Schulen blickt.

Kapitel 2

Über die deutsche und europäische Zusammenarbeit

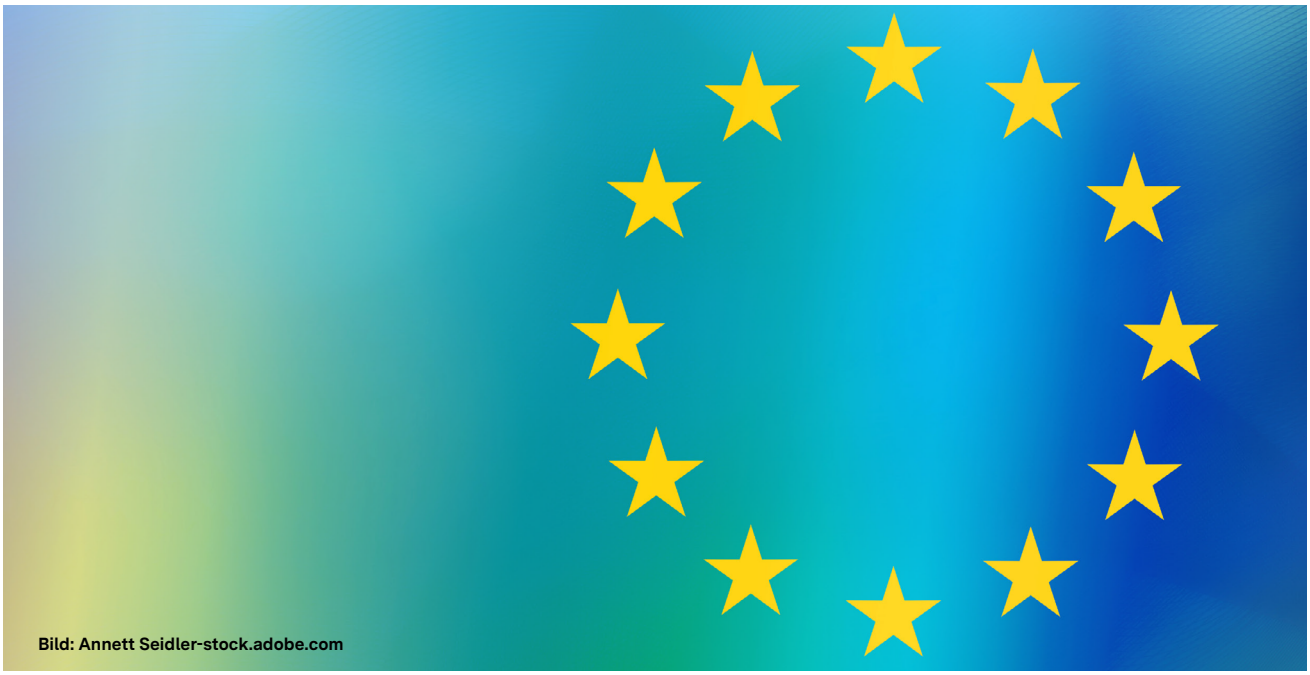


Bild: Annett Seidler-stock.adobe.com

2. Koordination in Europa und Deutschland

Wir erarbeiten europäische Leitlinien für die Bürger_innen und verantwortliche Stellen und beteiligen uns an koordinierten Maßnahmen. In Deutschland sind wir in der Datenschutzkonferenz aktiv, im Jahr 2026 haben wir dort den Vorsitz.

Art. 57 Abs.1 Buchst. b), d), g), i), t)

2.1. Europaweite Aktion zum Recht auf Löschung

Mit der sogenannten „schwäbischen Kehrwoche für Europa“, die wir bereits im Tätigkeitsbericht 2024 vorgestellt hatten (vgl. LfDI BW, 40. Tätigkeitsbericht Datenschutz 2024, S.41), haben wir den Anstoß für eine europaweite Schwerpunktsetzung beim Recht auf Löschung gegeben. Der Europäische Datenschutzausschuss (EDSA) hat auf unseren Vorschlag die praktische Umsetzung des Rechts auf Löschung gemäß Art. 17 DS-GVO als Thema seiner vierten koordinierten Durchsetzungsinitiative – Coordinated Enforcement Framework CEF – ausgewählt. Das CEF dient dem Ziel, eine kohärente Anwendung und Umsetzung der DS-GVO in Europa sicherzustellen und die Zusammenarbeit der Aufsichtsbehörden zu stärken. Nach bisherigen Aktionen zu Cloud-Diensten für öffentliche Stellen, zur Rolle von Datenschutzbeauftragten und zum Auskunftsrecht nach Art. 15 DS-GVO richtet sich der Fokus nun auf ein weiteres Betroffenenrecht, das im Beschwerdealltag aller europäischen Datenschutzbehörden eine zentrale Rolle spielt: das Recht auf Löschung bzw. „Recht auf Vergessenwerden“.

An der europäischen Aktion nahmen insgesamt 32 Datenschutzaufsichtsbehörden teil, darunter mehrere Landesdatenschutzbehörden in Deutschland sowie die Bundesbeauftragte. Neben der Tatsachenfeststellung („fact-finding“) als Ziel haben einige Aufsichtsbehörden auch formelle Untersuchungen eingeleitet, bereits laufende Untersuchungen fortgesetzt oder beabsichtigen auf Grundlage der gewonnenen Erkenntnisse, Maßnahmen zu ergreifen.

Kerninstrument der gemeinsamen Initiative ist ein europaweit abgestimmter Fragebogen zur Umsetzung des Rechts auf Löschung durch Verantwortliche. Der Fragebogen ist auf unserer Homepage online abrufbar und kann Verantwortlichen als Self-Check zur Selbstkontrolle zur Implementierung des Art. 17 DS-GVO und damit als „Realitätscheck“ dienen.

Im Rahmen der koordinierten Aktion haben wir einzelne öffentliche Stellen, Unternehmen sowie ausgewählte Einrichtungen aus besonders datenintensiven Sektoren – darunter insbesondere das Gesundheitswesen und der Bildungsbereich – befragt. Ziel war es, einen möglichst breiten und praxisnahen Überblick über Herausforderungen und Problemfelder bei der Umsetzung von Löschbegehren zu gewinnen. Ein besonderer Fokus lag zudem darauf, Best Practices zu identifizieren, insbesondere hinsichtlich organisatorischer Abläufe, interner Prozesse, eingesetzter technischer Werkzeuge sowie der praktischen Entscheidungsfindung bei komplexen Löschsituationen.

Die Ergebnisse der gemeinsamen Initiative werden im Rahmen des EDSA analysiert, ausgewertet und nach Abschluss zusammenfassend in einem Bericht veröffentlicht.

Mehr zur Digitalen Kehrwoche und dem Art. 17 Self-Check: https://www.baden-wuerttemberg.datenschutz.de/digitale-kehrwoche/

2.2. Social Media Expert Subgroup – Interplay Digital Services Act und DS-GVO

Der EDSA hat Leitlinien zum Zusammenspiel des DSA (Digital Services Act, kurz: DSA) und der DS-GVO veröffentlicht. Der DSA legt Hosting- und Vermittlungsdienstleistern eine Reihe von Erhebungs-, Überprüfungs- und Offenlegungspflichten, von denen einige auch den Datenschutz betreffen. Die nun veröffentlichten Leitlinien sollen eine einheitliche Auslegung und Anwendung des DSA und der DS-GVO sicherstellen. Wir waren federführend an der Erstellung der Leitlinien beteiligt.

Eine gemeinsame Auslegung beider Rechtsvorschriften ist nicht nur für Hosting- und Vermittlungsdienstleister wichtig. Auch die zuständigen Aufsichtsbehörden müssen den DSA und die DS-GVO zusammen berücksichtigen, damit Anbieter rechtssicher handeln können und die Rechte und Freiheiten von Personen, deren personenbezogene Daten verarbeitet werden, geschützt blei-

Infokasten

Leitlinien zum Zusammenspiel des DSA und DS-GVO: Guidelines 3/2025 on the interplay between the DSA and the GDPR: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/guidelines-32025-interplay-between-dsa-and-gdpr_en

Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005, ABl. L 149 S. 22, ELI: http://data.europa.eu/eli/dir/2005/29/oj

Siehe auch Beitrag „Irreführende Designs im Internet“, LfDI BW, 40. Tätigkeitsbericht Datenschutz 2024, Seite 36 ff.: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/03/TB_40_Datenschutz-2024_barrierefrei.pdf

ben. Darüber hinaus verweisen mehrere Bestimmungen des DSA ausdrücklich auf Konzepte der DS-GVO (z. B. Profiling und besondere Kategorien personenbezogener Daten). Es gibt somit zahlreiche Ähnlichkeiten und Überschneidungen zwischen der DS-GVO und dem DSA, was die Notwendigkeit von Leitlinien zu diesen Fragen unterstreicht – insbesondere im Hinblick auf die jeweiligen Verpflichtungen der verschiedenen Parteien, die beiden Rechtsrahmen unterliegen.

In den Leitlinien sind daher unter anderem die folgenden inhaltlichen Schwerpunkte zu finden:

- Die Erkennung und Beseitigung rechtswidriger Inhalte auf bspw. Online-Plattformen kann personenbezogene Daten betreffen. Die Leitlinien erklären, wann bei der Erkennung, Feststellung und Entfernung von rechtswidrigen Inhalten Art. 6 Abs.1 Buchst. c) oder Buchst. f) DS-GVO als datenschutzrechtliche Rechtsgrundlage zur Anwendung kommen können und nennen dafür Beispiele.
- Bei Melde- und Abhilfeverfahren dürfen Anbieter nur die notwendigen personenbezogenen Daten erheben. Zudem müssen meldende Personen nicht immer ihren Namen angeben, es sei denn, dies ist zur Bestimmung der Rechtswidrigkeit des Inhalts erforderlich. Das Beschwerderecht nach DSA berührt nicht die Rechte und Rechtsmittel der Betroffenen aus der DS-GVO gegenüber Anbietern von Online-Plattformen, sofern diese datenschutzrechtlich verantwortlich sind.
- Das Verbot für „Deceptive Design Patterns“ (irreführende Gestaltung) in Art. 25 DSA betrifft nur solche Praktiken, die nicht von der DS-GVO oder der Richtlinie über unlautere Geschäftspraktiken erfasst sind. Um festzustellen, ob ein Deceptive Design Pattern der DS-GVO unterliegt, ist es entscheidend, ob personenbezogene Daten verarbeitet werden und ob das Verhalten der Nutzenden durch diese Datenverarbeitung beeinflusst wird. Dies wird durch Beispiele ergänzt, in denen Deceptive Design Patterns unter die DS-GVO fallen oder nicht.

Eine To-Do Liste in Postkartenform. Illustration: T. Damjanović, LfDI BW

- Plattformen müssen transparent über Werbung informieren. Werbung, die auf Profiling mit besonderen Kategorien personenbezogener Daten (Art. 9 DS-GVO) basiert, ist zusätzlich zu den bestehenden DS-GVO-Verboten unter Art. 9 Abs.1 und Art. 22 Abs.4 DS-GVO verboten – selbst wenn eine Ausnahme nach Art. 9 Abs.2 DS-GVO vorliegt.
- Die Verarbeitung von Nutzendendaten zur Personalisierung kann problematisch sein, z.B. hinsichtlich der Richtigkeit, Transparenz und der mit umfangreichen Datensätzen sowie sensiblen Daten verbundenen Risiken. Empfehlungssysteme (Recommender Systems) können in manchen Fällen eine Entscheidung im Sinne von Art. 22 Abs. 1 DS-GVO sein. Nutzenden sollten echte Wahlmöglichkeiten gegeben werden. Sie sollten nicht zu einem profilbasierten Empfehlungssystem gedrängt werden (Nudging). Wenn sie eine nicht profilbasierte Option wählen, darf die Plattform kein Profiling betreiben.
- Der DSA enthält Regelungen zum Schutz von Kindern. Demnach müssen Online-Plattformen geeignete und verhältnismäßige Maßnahmen ergreifen, um ein hohes Maß an Privatsphäre, Sicherheit und Schutz von Minderjährigen innerhalb ihres Dienstes zu gewährleisten. Die Leitlinien klären, dass Art. 28 Abs.1 und 2 DSA eine rechtliche Verpflichtung gemäß Art. 6 Abs.1 Buchst. c) DS-GVO darstellen kann, sofern die Verarbeitung erforderlich und verhältnismäßig ist. Dies ist durch den Betreiber der Online-Plattform nachzuweisen. Anbieter sollten Mechanismen zur Altersbestimmung vermeiden, die zur eindeutigen Identifizierung führen. Zudem sollten keine Altersdaten dauerhaft gespeichert werden, insbesondere wenn die Information ausreicht, ob Zugang zur Online-Plattform gewährt wird oder nicht.
- Systemische Risiken bei großen Plattformen: Sehr große Online-Plattformen und sehr große Online-Suchmaschinen müssen Risiken für Grundrechte – auch Datenschutzrisiken – berücksichtigen und entsprechende Maßnahmen umsetzen. Dabei können Datenschutzprinzipien wie Datenminimierung und Privacy by Design helfen. Bei erkannten Risiken ist oft eine Datenschutz-Folgenabschätzung erforderlich.
- Verhaltenskodizes und Zusammenarbeit der Aufsichtsbehörden: Die im Rahmen des DSA entstehenden Regeln sollten in Abstimmung mit den Datenschutzbehörden entwickelt werden. Eine Koordination zwischen den DSA-Aufsichtsbehörden, der EU-Kommission und den Datenschutzbehörden ist wichtig, um widersprüchliche Entscheidungen zu vermeiden.

Die Kernaussage der Leitlinien lautet: DSA-Pflichten und DS-GVO-Rechte müssen zusammen gedacht werden. Die Leitlinien sollen Behörden und Anbieter anleiten, damit Datenschutzrechte gewahrt bleiben und Rechtsklarheit besteht.

Illustration: Y. Dwiputri

2.3. Datenschutz und Künstliche Intelligenz – Arbeitskreis KI

Wir haben gemeinsam mit dem LfDI Rheinland-Pfalz den Vorsitz des Anfang des Jahres 2025 eingerichteten Arbeitskreises „Künstliche Intelligenz“ (AK KI) der Datenschutzkonferenz (DSK). Hier bereiten wir unter anderem Orientierungshilfen für die DSK vor. Solche Arbeitspapiere setzen bundesweit einheitliche Standards zu datenschutzrechtlichen Fragen beim Einsatz von KI.

Es dürfte unstrittig sein, dass der Einsatz von Künstlicher Intelligenz (KI) – ganz gleich wie klug, sinnvoll oder schädlich man sie im Einzelfall findet – in den kommenden Jahren die Entwicklung der Digitalisierung dominieren wird. Also haben wir als DSK reagiert und ein Fachgremium geschaffen, welches das Ziel hat, Orientierung zu bieten. Die erste Orientierungshilfe war dann auch ein voller Erfolg – sie handelt davon, wie Verantwortliche generative KI-Modelle datenschutzrechtlich verbessern können (siehe Beitrag zur RAG-Methode).

Wir haben in diesem Arbeitskreis auch ein dauerhaftes Gremium für Forschung und neuere Entwicklungen im Bereich KI sowie ein Gremium für Entwicklungen auf EU-Ebene und weltweit zum Thema KI eingerichtet. Der Bedarf für spezifische Gremien hat sich in den letzten Jahren deutlich gezeigt. Die Verfolgung der sehr dynamischen Entwicklungen im Bereich KI – auch im Zusammenhang mit den zahlreichen weiteren digitalen Rechtsakten der EU – kann durch die gemeinsame Arbeit innerhalb der DSK geleistet werden. Über die DSK können wir praxisnahe Lösungsansätze für Verantwortliche entwickeln.

Wir befassen uns in dem Gremium mit der Frage der Umsetzung der Betroffenenrechte, insbesondere mit der Sicherstellung der Transparenz bei der Verarbeitung personenbezogener Daten mit einer KI. Auch geht es hier um die datenschutzrechtlichen Anforderungen beim Training der KI und dem Umgang mit einem rechtswidrig trainierten KI-Modell (vgl. EDSA-Stellungnahme 28/2024). Schließlich haben wir das Aufgabengebiet erweitert und uns mit der Frage befasst, wie sich RAG auf ein generatives KI-System auswirkt. Hierzu haben wir als DSK dann auch eine Orientierungshilfe veröffentlicht.

Im Verlauf des Jahres hat sich insbesondere gezeigt, dass das Thema KI als Querschnittsthema für andere Arbeitskreise der DSK von grundlegender Bedeutung ist. Für den öffentlichen Bereich gibt es in den Bundesländern unterschiedliche Landesdatenschutzgesetze und der Einsatz von KI in der öffentlichen Verwaltung ist daher von einer besonderen rechtlichen Vielfalt geprägt. Zudem sind in verschiedenen Bundesländern und auf Bundesebene Anpassungen der datenschutzrechtlichen Vorschriften geplant oder bereits erfolgt, sodass sich in diesem Bereich viel bewegt. Daher soll mit dem Arbeitskreis Verwaltung eine gemeinsame Arbeitsgruppe etabliert werden, um die datenschutzrechtliche Rechtsgrundlage für den Einsatz von KI im öffentlichen Bereich im Detail zu untersuchen und öffentliche Stellen bei einem datenschutzrechtskonformen KI-Einsatz zu unterstützen.

Der Arbeitskreis Künstliche Intelligenz der DSK hat sich als dauerhaftes Gremium etabliert. Durch regelmäßige Sitzungen und mehrere Arbeitsgruppen verfolgt er die dynamische Entwicklung von KI und die damit verbundenen datenschutzrechtlichen Herausforderungen. Ein Schwerpunkt liegt auf praxisnahen Orientierungshilfen, die auch in enger Zusammenarbeit mit weiteren DSK-Arbeitskreisen, wie dem AK Verwaltung für den öffentlichen Bereich, erarbeitet werden.

Mehr zur RAG-Methode:
https://www.baden-wuerttemberg.datenschutz.de/dsk-oh-rag-pm/

2.4. RAG-Methode: generative KI-Modelle verlässlicher gestalten

Der Arbeitskreis KI (AK KI) der DSK hat im Oktober 2025 eine Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode veröffentlicht (RAG: Retrieval Augmented Generation). Mithilfe der RAG-Methode soll die Genauigkeit, Nachvollziehbarkeit und Verlässlichkeit der Ausgaben generativer KI-Systeme erhöht werden, während gleichzeitig die Wahrscheinlichkeit für Halluzinationen und unrichtige Ausgaben verringert wird. Dies soll durch die Erweiterung des Eingabeprompts um domänenspezifisches Wissen aus Unternehmen oder Behörden erreicht werden. In der Orientierungshilfe werden insbesondere die Auswirkungen der RAG-Methode auf die Grundsätze der DS-GVO in KI-Systemen untersucht.

In der Orientierungshilfe werden RAG-Systeme mit Embeddings und Vektordatenbanken behandelt, da sie eine an der Semantik orientierte Suche in Referenzdokumenten ermöglichen, die in der Praxis inzwischen häufig eingesetzt wird. Während ohne RAG-Methode ein textgenerierendes Sprachmodell aus der Eingabe mit Hilfe des textgenerierenden Sprachmodells eine Ausgabe erzeugt (siehe Abb. 1), wird mit der RAG-Methode die Eingabe erweitert (siehe Abb. 2).

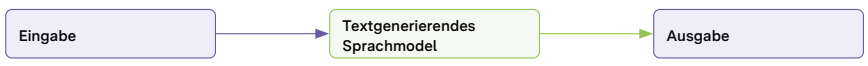
Dazu werden mithilfe einer (semantischen) Suche (Retrieval) aus den Referenzdokumenten inhaltlich passende Textabschnitte identifiziert, die Eingabe erweitert (Augmentation) und mit einem textgenerierenden Sprachmodell eine Ausgabe erzeugt (Generation). Damit erklärt sich die Abkürzung RAG (Retrieval Augmented Generation). (Eine detaillierte Erklärung der einzelnen Schritte findet sich in der Orientierungshilfe.)

> ☝ Weitere Informationen
>
> Wichtig: Die datenschutzrechtliche Beurteilung des Trainings der verwendeten LLMs bleibt durch ein RAG unberührt. Ein rechtswidrig trainiertes KI-Modell bleibt auch in einem RAG-System rechtswidrig.

Die RAG-Methode ist datenschutzrechtlich relevant, da sich eine positive Wirkung auf die Richtigkeit (Reduktion von Halluzinationen) und Nachvollziehbarkeit der Ausgaben ergeben kann und die Vertraulichkeit und Integrität zusätzlich eingebundener personenbezogener Daten verbessert werden kann. In vielen Fällen ermöglicht RAG zudem den Einsatz eines textgenerierenden Sprachmodells (Large Language Model, LLM) on-premise und die Nutzung von KI-Modellen mit weniger umfangreichen Trainingsdaten. Dadurch sind u. a. weniger personenbezogene Daten aus dem KI-Modell extrahierbar.

Die Orientierungshilfe der DSK analysiert die Auswirkungen des Einsatzes der RAG-Methode auf die datenschutzrechtliche Bewertung generativer KI-Systeme unter Berücksichtigung der Grundsätze der DS-GVO (Art. 5 DS-GVO) und der Betroffenenrechte (Kapitel 3 DS-GVO). Im Folgenden sollen einige der relevanten Punkte dargestellt werden. Dabei kann RAG Halluzinationen reduzieren und die Richtigkeit der Ausgaben erhöhen, da diese in der Regel aus den Referenzdokumenten stammen. Zu beachten sind hierbei die Qualität der Referenzdokumente, die Datenaufbereitung und die regelmäßige Aktualisierung der Dokumente – ohne diese Punkte kann auch RAG keine korrekten Ergebnisse liefern. Auch kann eine Erhöhung der Transparenz in Bezug auf das eingesetzte LLM nicht erreicht werden, jedoch besteht Transparenz hinsichtlich der erweiterten Eingabe an das LLM, sofern die genutzten Textabschnitte der Referenzdokumente in der Ausgabe dokumentiert werden. Im RAG-System, d. h. insbesondere bei den Referenzdokumenten, können bewährte Maßnahmen wie Mandantentrennung/funktionale

Abb. 1 LLM ohne RAG



Trennung und Rechte- und Rollenkonzepte angewendet werden. Dadurch ist auch die Verarbeitung von Daten mit hohem Schutzbedarf (Art. 9 und 10 DS-GVO) denkbar. Auch die Zweckbindung kann technisch durch Mandantentrennung umgesetzt werden. Allerdings besteht die Gefahr einer Verletzung der Zweckbindung durch die Verkettung von Daten aus den Referenzdokumenten mit personenbezogenen Daten im LLM. Zudem kann der Umfang der in den Referenzdokumenten gespeicherten Daten bestimmt und kontrolliert werden. Diese Daten sind gezielt löschbar. Allerdings bleibt die Problematik der Löschung personenbezogener Daten im LLM bestehen.

Für die Verarbeitung personenbezogener Daten ist eine Rechtsgrundlage erforderlich.

„Bei RAG-Systemen ist zu beachten, dass bei einem ggf. rechtswidrig trainierten LLM unabhängig von der Integration im RAG-System das Training weiterhin rechtswidrig bleiben würde. Allerdings können einige der damit einhergehenden Risiken für die Rechte und Freiheiten von betroffenen Personen durch die Verwendung der RAG-Methode gemindert werden. Die konkrete Auswirkung eines RAG-Systems lässt sich jedoch nur im Einzelfall überprüfen. […] Sollten für den Einsatz eines KI-Systems ohne RAG-Methode die Voraussetzungen für eine datenschutzrechtliche Rechtsgrundlage nicht vorliegen, weil z. B. die Interessen der betroffenen Personen die Interessen des Verantwortlichen überwiegen, kann geprüft werden, ob durch den Einsatz der RAG-Methode risikomindernde Maßnahmen ergriffen werden können, die über die Maßnahmen hinausgehen, zu denen der Verantwortliche ohnehin gesetzlich verpflichtet ist“. (OH RAG, Abschnitt 3.6.)

Hervorzuheben ist hier, dass

„je nach Gestaltung, […] die Nutzung der RAG-Methode somit gegebenenfalls als eine von verschiedenen mitigierenden Maßnahmen im Sinne der EDSA-Stellungnahme 28/2024 erachtet werden [kann]“. (OH RAG, Abschnitt 4. Siehe auch EDSA-Stellungnahme 28/2024, Rn. 96 ff.; EDSA-Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR, Version 1.0, 8 October 2024, Rn. 57.)

Die RAG-Methode kann bestimmte Schwächen von KI-Systemen, wie beispielsweise Halluzinationen, reduzieren. Die jeweiligen Herausforderungen und Erleichterungen sind jedoch im Einzelfall zu prüfen. Unter Umständen kann die Nutzung der RAG-Methode als eine mitigierende Maßnahme im Sinne der EDSA-Stellungnahme 28/2024 betrachtet werden.

Infokasten

Pressemitteilung der Datenschutzkonferenz, vom 17.10.2025: DSK veröffentlicht Orientierungshilfe zu KI-Systemen mit Retrieval Augmented Generation (RAG): https://www.datenschutzkonferenz-online.de/media/pm/DSK_PM_OH-RAG-Systeme.pdf

Datenschutzkonferenz: Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode: https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf

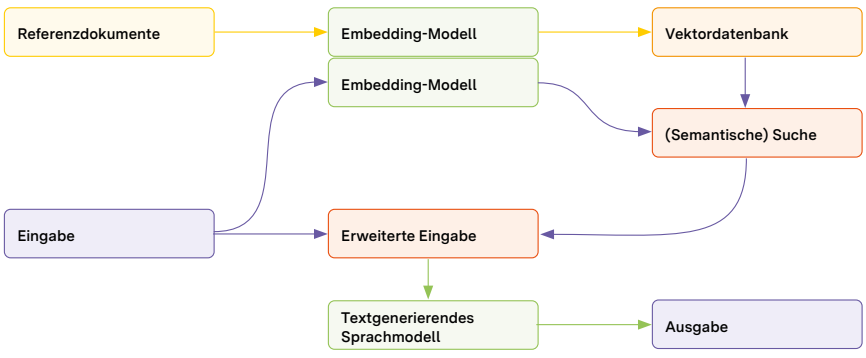
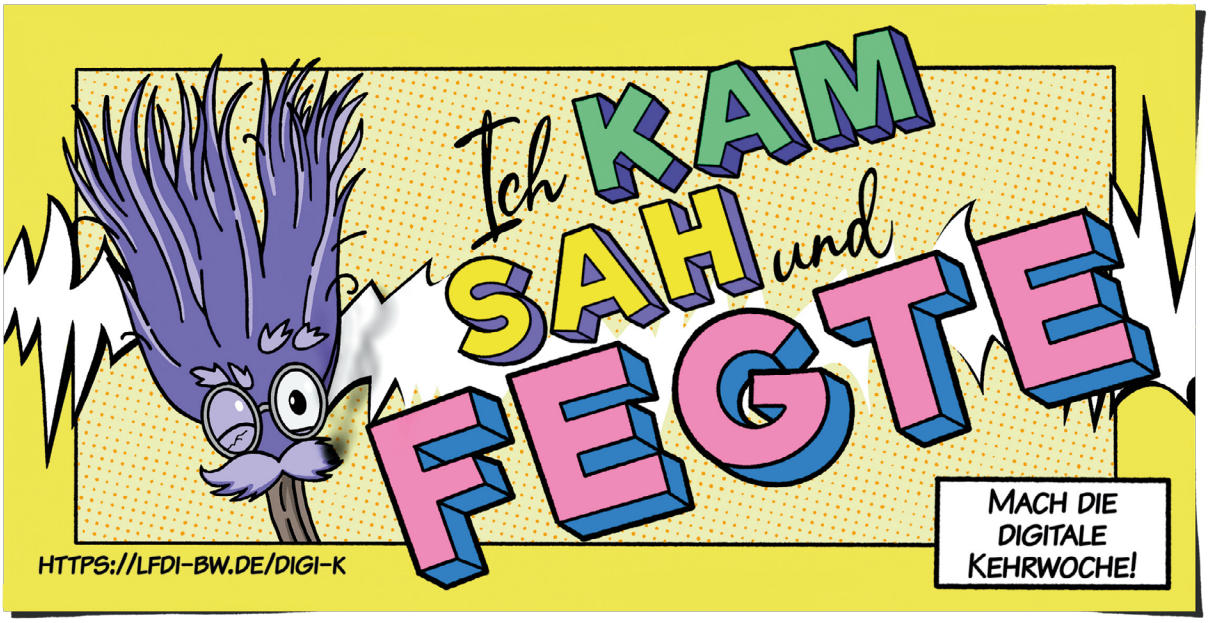


Abb. 2 LLM mit RAG



Sticker zur Digitalen Kehrwoche.
Illustration: T. Damjanović, LfDI BW

2.5. Digitale Kehrwoche mit Kehrolin – „Ich kam, sah und fegte“

Um auch die Bürgerschaft für das Thema Löschen zu sensibilisieren und Datenschutz einfach und praktisch zu machen, rief der Landesbeauftragte die „Digitale Kehrwoche“ aus. Ziel der Aktion ist, Menschen dazu einzuladen, sich ab und an zu fragen, ob man alles, was man auf seinem PC, Smartphone oder in der Cloud gespeichert hat, tatsächlich noch braucht – und wenn nicht, auch mal zu löschen. Das urschwäbische Prinzip der Kehrwoche, das bundesweit bekannt ist, kann auch für die digitale Welt Vorbild sein. Unsere Kehrwoche in Baden-Württemberg operationalisiert auf sehr praktische und traditionsbewusste Weise Themen zu Artikel 17 DS-GVO.

Um das Thema Löschen auch im privaten Umfeld stärker präsent zu machen, haben wir eine Bucket List in Form einer Postkarte für den privaten Gebrauch erstellt. Der englische Begriff Bucket List bezeichnet eine Liste von Dingen, die man noch tun möchte, bevor man ein bestimmtes Alter erreicht. Gleichzeitig bezeichnet bucket schlicht einen Eimer.

Die Bucket List zählt fünf Aufgaben auf, die man ohne viel Aufwand während einer Woche erledigen kann, um den eigenen Datenmüll etwas zu reduzieren. Die Betonung liegt auf einem einfachen Format, schnell sichtbaren Erfolgen und einem gewissen Augenzwinkern.

Infokasten

Digitale Kehrwoche – Bucket List: https://www.baden-wuerttemberg.datenschutz.de/digitale-kehrwoche-bucket-list/

Ein schöner Anlass, um das Thema Löschen sowie das individuelle Recht auf Löschung nach Artikel 17 DS-GVO direkt mit Bürger_innen zu diskutieren bot das „Fest der digitalen Freiheit – Aktionstag pro Datenschutz und contra Fake News“, wo wir den Vortrag „Meine Rechte im Datenschutz … und was die Kehrwoche damit zu tun hat“ gehalten haben (s. Kap. 4.4.5.).

Unsere Aktionen zur Digitalen Kehrwoche richteten sich gleichermaßen an verantwortliche Stellen. Neben den Ergebnissen aus dem CEF 2025 (siehe oben unter 2.1.), referierten wir auf der BvD-Herbstkonferenz 2025 zu den „Herausforderungen der Digitalen Kehrwoche“ (s. Kap. 4.1.). Auch dieses Format bot einen wertvollen Rahmen, um die Praxiserfahrungen verantwortlicher Stellen mit Artikel 17 DS-GVO direkt mit diesen zu besprechen.

Digitale Kehrwoche schon gemacht?

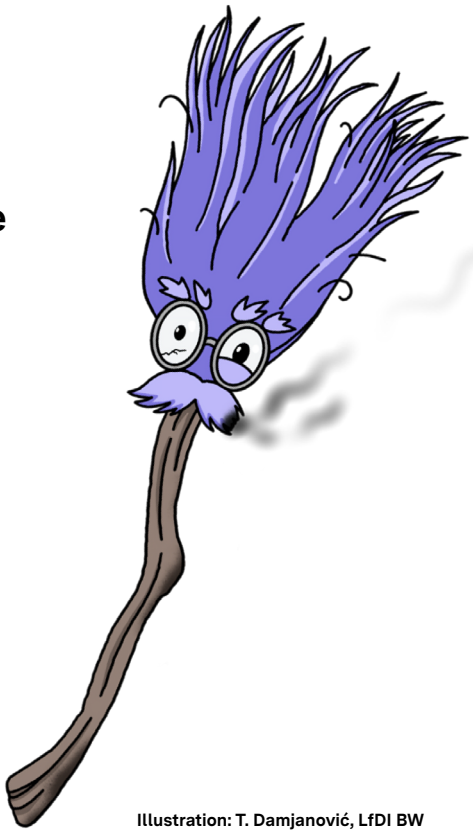


Illustration: T. Damjanović, LfDI BW

Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA)

QR-Code scannen

https://www.baden-wuerttemberg.datenschutz.de/onkida

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Kapitel 3

Gesetze und Verwaltungs-vorschriften: Stellungnahmen

3. Gesetze und Verwaltungsvorschriften: Stellungnahmen

Eine wesentliche Aufgabe von uns ist es, die Landesregierung, den Landtag und die Verwaltung im Zuge von Gesetzgebungsverfahren und bei der Erarbeitung von Verwaltungsvorschriften zu beraten.

3.1. Frühzeitige Beteiligung ermöglicht Unterstützung

Art. 57 Abs.1 Buchst. c) DS-GVO

Nach Art. 57 Abs.1 Buchst. c) DS-GVO und Art. 36 Abs.4 DS-GVO ist es Aufgabe der Datenschutzaufsichtsbehörden, das Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung zu beraten. Diese Beratung ist wichtiger Baustein im Grundrechtsschutz, damit insbesondere in grundrechtssensiblen Bereichen mit erheblicher Eingriffsintensität der Gesetzgeber nicht nur den verfassungsrechtlichen Vorgaben (z.B. Wesentlichkeitstheorie, Übermaßverbot), sondern auch den europarechtlichen Vorgaben genügt. Soweit nämlich die DS-GVO Öffnungsklauseln für den nationalen Gesetzgeber enthält, verlangt sie von diesem beispielsweise „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ (Art. 9 Abs.2 Buchst. i) DS-GVO), „Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung“ (Art. 6 Abs.3 Satz 3 DS-GVO) oder „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person“ (Art. 88 Abs.2 DS-GVO).

In Baden-Württemberg ist die Beteiligung ergänzend zur DS-GVO insbesondere in § 26 Absatz 2 LDSG, § 8 Abs.2 Nr. 5 LDSG-JB, § 98 Abs.1 Nr. 3 PolG und der Verwaltungsvorschrift 'Regelungen' formuliert. Danach beteiligen die Ministerien den Landesbeauftragten rechtzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen.

Diese Aufgabe besteht für uns auch außerhalb des Anwendungsbereichs der DS-GVO. Die Schwester der DS-GVO, die europäische Richtlinie 2016/680 ("JI-RL"), sieht in ihrem Art. 46 Abs.1 Buchst. c) gleichfalls die Beratung der Legislative und Exekutive vor. Die Richtlinie betrifft vor allem den Bereich der Gefahrenabwehr, der Strafverfolgung und der Ordnungswidrigkeiten. Die nationale Umsetzung der Aufgabe der Beratung findet sich dementsprechend im Polizeigesetz (PolG) und dem Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden (LDSG-JB).

Insgesamt wurden wir im Jahr 2025 beteiligt bei 142 Gesetzgebungsverfahren sowie Verordnungen und Verwaltungsvorschriften. Eine frühzeitige Einbindung in den Gesetzgebungsprozess ist für uns wichtig, damit wir die Verfahren datenschutzrechtlich unterstützend begleiten können. Im Folgenden stellen wir einige Beispiele aus diesem Beratungsbereich vor.

3.2. Verfahrensübergreifende Recherche- und Analyseplattform

§ 98 Abs.1 Nr. 3 PolG

Mit der Änderung des Polizeigesetzes vom 18. November 2025 hat der Landesgesetzgeber für die Polizei Baden-Württemberg die Erlaubnis zur verfahrensübergreifenden Datenrecherche und -analyse geschaffen. Vor und in dem Gesetzgebungsverfahren haben wir dazu beraten. Darüber hinaus beraten wir auch zur konkreten Umsetzung, also der Einrichtung und Nutzung von entsprechender Hard- und Software.

Es steht außer Frage, dass die Polizei in Zeiten zunehmender Digitalisierung und immer schneller voranschreitender technischer Entwicklungen angemessene Ermittlungsbefugnisse und -mittel benötigt. Dazu gehört auch die Möglichkeit, vorhandene Daten verfahrensübergreifend durchsuchen zu können. Dass der Gesetzgeber grundsätzlich eine solche Erlaubnis schaffen darf, steht auch spätestens mit der Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 zu HessenDATA außer Zweifel.

Allerdings muss eine solche Erlaubnis verfassungsrechtlichen Anforderungen entsprechen und insbesondere die Art und den Umfang der Daten sowie die Verarbeitungsmethode klar regeln. Der Ende des Jahres 2025 neu geschaffene § 47a PolG ist eine umfangreiche und komplexe Regelung, die z. B. das Eingriffsgewicht der Maßnahme entsprechend der Rechtsprechung des Bundesverfassungsgerichts dadurch steuert, dass für verschiedene Konstellationen unterschiedlich umfangreiche Datenmengen durchsucht werden dürfen und / oder bestimmte Informationsquellen ausgeschlossen sind. Dennoch haben wir Zweifel an der Ausgestaltung der Norm, da aus unserer Sicht wesentliche Faktoren entweder gar nicht oder nur unzureichend durch den Gesetzgeber bestimmt werden. Dies ist aus unserer Sicht heikel, da mit der Regelung eine Maßnahme von erheblicher Eingriffsintensität geschaffen wurde, über deren Einsatzmöglichkeiten nun in wesentlichen Hinsichten die Exekutive entscheidet:

1. Welche Daten dürfen durchsucht werden

Der Gesetzgeber hat die durchsuch- und analysierbaren Daten im Wesentlichen so definiert, dass er die polizeilichen Systemarten benennt, deren Daten genutzt werden dürfen („Zum Zweck der automatisierten Datenanalyse können eigene Vorgangsdaten, Falldaten, Daten aus polizeilichen Auskunftssystemen und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden."). Das führt allerdings dazu, dass die Exekutive selbst entscheidet, welche Daten zur Recherche und Analyse bereitgestellt werden: So kann also bspw. – je nach technischer Umsetzung – grundsätzlich jede im „Fallbearbeitungssystem" abgelegte Information für die landesweite Recherche und Analyse verfügbar werden.

2. Wessen Daten dürfen durchsucht werden / Schutz „Unbeteiligter"

„Unbeteiligte" werden von der Vorschrift zwar gesondert geschützt („Zum Schutz unbeteiligter Personen werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen"; „die Einbeziehung von Daten unbeteiligter Personen [sei] möglichst zu vermeiden"). Allerdings wird weder im Gesetzeswortlaut, noch in der -begründung klargestellt, wer „Unbeteiligter" ist.

Infokasten

Unsere umfassenden Stellungnahmen sind Teil der Landtags-Drucksache 17/9478, S. 117 ff.: https://www.landtag-bw.de/resource/blob/596660/4e61c8adee1d16d9d2d8017a-1bee8e0e/17_9478_D.pdf

Die Stellungnahmen stehen auch in den Shownotes unserer 49. Podcast-Folge „Videoüberwachung und VeRA": https://www.baden-wuerttemberg.datenschutz.de/datenfreiheit-49-videoueberwachung-vera/

Die mündliche Stellungnahme im Rahmen der Sitzung des Petitionsausschusses, vom 6. November 2025: https://www.landtag-bw.de/de/mediathek/videos/oea-peta-vom-6-november-2025-602650 (ab Minute 3).

3. Wie dürfen die Daten analysiert werden / auf welche Weise darf künstliche Intelligenz eingesetzt werden

Der Wortlaut der Regelung selbst sieht nur vor, dass der „Polizeivollzugsdienst [...] personenbezogene Daten [...] automatisiert [...] bewerten“ kann, wobei sicherzustellen ist, „dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden“ und eine „abschließende Bewertung der bereitgestellten Informationen und die Entscheidung über weitere Maßnahmen [...] durch den Polizeivollzugsdienst getroffen [werden]“. Aus unserer Sicht bleibt damit zu offen, welches Ziel eine automatisierte Bewertung haben darf, welche „Entscheidungen“ automatisiert getroffen werden dürfen und welche nicht.

Bild: Daniela Zampieri / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Infokasten

In ihrer Entschließung vom 17. September 2025 hat sich die Datenschutzkonferenz (DSK) zum Einsatz automatisierter Recherche- und Analysemethoden in der polizeilichen Arbeit geäußert. Darin fordert sie, dass solche Systeme nur auf Grundlage verfassungskonformer spezifischer Rechtsgrundlagen eingesetzt werden und die digitale Souveränität gewährleistet wird. Eine Chance für eine souveräne Lösung, ggf. unter Einbindung von Open Source-Produkten, ist das IT-Großprojekt „Polizei 20/20“, das die DSK seit mehreren Jahren berät.

DSK-Entschließung: „Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten", vom 17. September 2025: https://www.datenschutzkonferenz-online.de/media/en/2025-09-17_DSK-Entschliessung_Automatisierte-Datenanalyse.pdf

Im Januar 2026 forderte die DSK in einer Entschließung klare gesetzliche Grundlagen für den Betrieb des P20-Datenhauses: https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_P20-Datenhaus.pdf

Die Beratung zur technischen Umsetzung der Datenanalyse haben wir bereits 2025 begonnen. Allerdings lag uns bis zum Jahresende die Verwaltungsvorschrift noch nicht vor, welche nach § 47a Abs. 4, 5 und 6 PolG wichtige datenschutzrechtliche Rahmenbedingungen für die Umsetzung festlegt. Darin sollen beispielsweise Konzepte zu Rechten und Rollen der nutzenden Personen und zur Kategorisierung der Daten ausgewiesen werden. Letzteres dürfte beispielsweise für die Frage entscheidend sein, wer „unbeteiligte Person" sein soll und wer nicht.

Grundsätzlich ist beim Einsatz privatwirtschaftlicher Dienstleister durch öffentliche Stellen – insbesondere die Polizei – entscheidend, dass deren Handeln hinreichend engmaschig kontrolliert und geprüft wird.

Wir kritisieren die neue Regelung zur Datenanalyse im Polizeigesetz: wichtige Weichen werden nicht durch den Gesetzgeber gestellt, sondern der Exekutive überlassen, z. B. im Hinblick auf den Einsatz Künstlicher Intelligenz. Die Beratung zur konkreten technischen Umsetzung hat gerade erst begonnen.

3.3. Update Standortdaten beim Notruf 110

§ 98 Abs. 1 Nr. 3 Polizeigesetz

Infolge unserer Beratung hat der Landtag ein Gesetz zur automatisierten Erhebung von Notrufdaten erlassen (verkündet im Gesetzblatt für BW 2025, Nr. 117 vom 18.11.2025). Das ist ein wichtiger Beitrag zur Rechtssicherheit.

In unserem vergangenen Tätigkeitsbericht hatten wir über unsere Beratung und Rechtsauffassung zum Einsatz von Advanced Mobile Location („AML") beim Wählen der 110 berichtet. Zusammengefasst war es erforderlich, eine eigene gesetzliche Regelung für den Einsatz dieser neuen Technologie zu schaffen, weil – anders als dies bisher der Fall war – durch sie nun bei jeglichem Anwählen der 110 ein Standortdatum der anrufenden Person durch die Polizei erhoben wird.

Dieser Automatismus ohne Einschätzungsspielraum, ob die Daten überhaupt tatsächlich benötigt werden, konnte nicht durch die bestehenden Regelungen abgebildet werden.

Infokasten

Näheres dazu siehe „Standortdaten beim Notruf 110", LfDI BW, 40. Tätigkeitsbericht Datenschutz 2024, S. 43 ff: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/03/TB_40_Datenschutz-2024_barrierefrei.pdf

LfDI-Stellungnahme zum Entwurf: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/08/Stellungnahme-03_2025-PolG-E.pdf

Wir freuen uns, dass das Innenministerium dies aufgegriffen und für den Landtag einen Gesetzesentwurf ausgearbeitet hat. Mit der Entscheidung des Gesetzgebers für § 45a Polizeigesetz wurde nunmehr eine rechtssichere Abwägung zwischen dem Recht auf Informationelle Selbstbestimmung der Anrufenden sowie dem Erfordernis effektiver Rettungsmöglichkeiten für die Polizei getroffen.

Datenschutz heißt: angemessener Ausgleich zwischen dem Schutz personenbezogener Daten und anderen legitimen Interessen. Insbesondere beim Einsatz neuer Technologien durch die Polizei kann dies wegen des Rechtsstaatsprinzips und der Gewaltenteilung bedeuten, dass die Legislative diese Abwägungsentscheidung ausdrücklich in Form einer konkreten gesetzlichen Erlaubnis treffen muss.

3.4. Streaming von Gremiensitzungen jetzt möglich

Art. 57 Abs.1 Buchst. c) DS-GVO

Bisher galt, dass Gemeinderats- und Kreistagssitzungen nur auf Grundlage von Einwilligungen aller betroffenen Personen gefilmt und ins Internet gestreamt werden durften. Mit der Änderung der Gemeindeordnung (GemO) und der Landkreisordnung (LKrO) hat der Gesetzgeber nun dafür eine Satzungsbefugnis geschaffen. Hat eine Gemeinde oder ein Landkreis eine entsprechende Satzung, braucht es folglich keine Einwilligung mehr. Wir empfehlen, klare Regelungen in der Satzung zu treffen – und die technischen und organisatorischen Schutzmaßnahmen nicht zu vergessen.

Kommunalpolitische Entscheidungen betreffen Bürger_innen jeden Tag und vermutlich mehr, als es vielen bewusst ist. Das Anliegen, die Teilhabe an diesem wichtigen demokratischen Prozess durch eine Übertragung von Gremiensitzungen ins Internet zu vereinfachen und mit dem Recht auf Informationelle Selbstbestimmung der betroffenen Personen in einen angemessenen Ausgleich zu bringen, haben wir sehr gerne von Anfang an unterstützt. Frühzeitig hatte uns das Innenministerium zu einem entsprechenden Gesetzgebungsvorhaben zur Beratung hinzugezogen (s. auch Koalitionsvertrag „Jetzt für Morgen“ von Bündnis 90 / Die Grünen Baden-Württemberg und der CDU Baden-Württemberg, S. 95).

Da es früher keine gesetzliche Grundlage für die Aufzeichnung und Veröffentlichung der Gremiensitzungen gab, mussten in der Vergangenheit alle betroffenen Personen im Sinne des Art. 6 Abs.1 Buchst. a) DS-GVO einwilligen. Mit Inkrafttreten des Gesetzes zur Änderung kommunalrechtlicher und weiterer Vorschriften vom 22. Juli 2025 hat der Gesetzgeber nun eine Satzungsbefugnis geschaffen. Die neuen Vorschriften in der GemO und LKrO waren erforderlich, da Gemeinden und Landkreise zwar für innere Angelegenheiten selbstständig Regelungen erlassen dürfen. Greifen diese Regelungen allerdings in Grundrechte ein, muss die Erlaubnis zu dem speziellen Grundrechtseingriff zunächst durch den Gesetzgeber erteilt werden – und dies ist nunmehr mit § 35 Abs. 3 GemO und § 30 Abs. 2 LKrO erfolgt. Die allgemeine Ermächtigung zum Erlass von Satzungen nach Art. 28 Abs. 2 Satz 1 Grundgesetz (GG) und § 4 Abs. 1 GemO hätten nicht ausgereicht. Ist eine wirksame Satzung in Kraft, kommt es folglich nicht mehr auf die Einwilligung der betroffenen Personen an, die Satzung selbst ist die Rechtsgrundlage für die Verarbeitungsvorgänge.

Zur datenschutzkonformen Umsetzung empfehlen wir insbesondere Folgendes klar zu regeln:

1. Welche Personengruppen sind betroffen?

Die Satzungsbefugnis bezieht sich nur auf den Eingriff in die Grundrechte der Gremiumsmitglieder und Vorsitzenden, insbesondere Beschäftigte der Verwaltungsbehörden oder Bürger_innen dürfen weiterhin nur auf Grundlage wirksamer Einwilligungen aufgezeichnet und veröffentlicht werden. Bei Einwilligungen, insbesondere in einem Über-Unterordnungsverhältnis, wie dies zwischen Beschäftigten und ihren Arbeitgeber_innen sowie Bürger_innen und dem Staat der Fall ist, ist die Freiwilligkeit einer Einwilligung sorgfältigst zu prüfen. Das bedeutet vor allem, dass den betroffenen Personen keine negativen Konsequenzen drohen dürfen, wenn sie die Einwilligung verweigern, und dass konkrete Möglichkeiten bestehen müssen, um an der Sitzung teilzunehmen, Fragen zu stellen oder Stellungnahmen abzugeben, ohne gefilmt und übertragen zu werden. Bei Beschäftigten der Kommunalverwaltung dürfen insbesondere keine negativen beruflichen Konsequenzen drohen, wenn die Einwilligung verweigert wird.

2. Welche Verarbeitungsvorgänge sollen stattfinden?

Die Satzungsgeber können darüber entscheiden, auf welche Weise sie die Teilhabe an der Sitzung durch Veröffentlichung ermöglichen wollen. Denkbar sind verschiedene Arten der Umsetzung, z. B. die Aufzeichnung alleinig des Tons oder von Ton und Bild sowie die Veröffentlichung alleinig für die Dauer der tatsächlichen Sitzung (also als Live-Stream) oder die Veröffentlichung auf Dauer/ für ein bestimmtes Zeitfenster (also als On-Demand-Stream). Wichtig ist, alle angestrebten Verarbeitungsvorgänge in der Satzung zu regeln, also auch die interne Speicherung der Aufzeichnung, bzw. dessen Löschung und die Dauer der Veröffentlichung. Konkret sollten mindestens die folgenden Verarbeitungsvorgänge bezeichnet und geregelt sein:

- Erhebung/Aufzeichnung welcher Daten (Bild oder Ton oder beides?)
- interne Speicherung und deren Dauer, bzw. Löschzeitpunkt
- Offenlegung der Aufzeichnung/ Veröffentlichung auf welche Weise, bzw. Dauer der Verfügbarkeit (Live-Stream oder On-Demand-Stream?)

Möglich ist es selbstverständlich auch, in der Satzung Differenzierungen vorzunehmen, bspw. zu regeln, dass grundsätzlich ein Live-Streaming erfolgt, aber durch eine Abstimmung eine längere Verfügbarkeit erwirkt werden kann, wenn Themen von besonderer Tragweite Gegenstand der Sitzung sind und dem besonderen öffentlichen Interesse daran Rechnung getragen werden soll.

Die Konzeption des Gesetzgebers, ein Streaming durch eine Satzungsbefugnis zu erlauben, überlässt die Abwägungsentscheidung zwischen Teilhabemöglichkeit an demokratischen Entscheidungsprozessen, Transparenz und den Grundrechten der betroffenen Personen den Satzungsgebern vor Ort. Dies ist aus unserer Sicht sinnvoll, da es ermöglicht, auf örtliche Begebenheiten und Umstände einzugehen. Die Abwägung kann folglich und sollte unseres Erachtens offen diskutiert und dann im Rahmen des Entscheidungs- und Einschätzungsspielraums der Gemeinderäte und Kreistage entschieden werden.

Wichtig dabei ist eine Abwägung der Zwecke und die Frage, was zur Erreichung dieser Zwecke erforderlich ist. Nach unserer Auffassung dient die Aufzeichnung und Veröffentlichung in erster Linie dazu, Personen die Teilnahme an der Gremiensitzung zu ermöglichen, die nicht vor Ort sein können. Der Zweck ist folglich nicht, ein Archiv jeglichen Entscheidungsprozesses anzulegen. Die wesentlichen Inhalte einer Sitzung werden ohnehin nach § 38 GemO in der Niederschrift festgehalten, die wiederum für alle Einwohner_innen einsehbar ist. Unsere Empfehlung geht deshalb dahin, nur ein Live-Streaming vorzusehen oder die automatisierte Löschung einer online gestellten Aufzeichnung mit Beginn der jeweils nächsten Sitzung einzurichten.

Eine Grenze für die Speicherung besteht allerdings jedenfalls dann, wenn keine Veröffentlichung (mehr) stattfindet. Gemeint ist: auch intern müssen die Auf-

Infokasten

Koalitionsvertrag „Jetzt für Morgen“ von Bündnis 90 / Die Grünen Baden-Württemberg und der CDU Baden-Württemberg, S. 95: https://www.baden-wuerttemberg.de/de/regierung/koalitionsvertrag-fuer-baden-wuerttemberg

LfDI-Handreichung zur Einbindung von Videos in eigene Webseiten: https://www.baden-wuerttemberg.datenschutz.de/videos-einbinden/

Unser Beitrag im 37. Tätigkeitsbericht Datenschutz 2021 auf S. 82 ist mit dem hiesigen Beitrag im Hinblick auf die Rechtsgrundlage überholt, nicht aber im Hinblick auf die weiteren dort genannten Vorgaben z. T. Online-Streaming von Gemeinderatssitzungen: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf

Das Kompetenzteam „Datenschutz“ des IT-Planungsrats erarbeitet derzeit (Stand 09/2025) eine Web-Applikation für einen Rechtsgrundlagengenerator, der ggf. zur Erstellung der Satzung hilfreich ist. Eine Vorlage kann bereits jetzt abgerufen werden unter https://www.it-planungsrat.de/der-it-planungsrat/strategische-schwerpunktthemen/schwerpunktthema-datennutzung

Außerdem noch der Hinweis: In den geänderten Gesetzen wurde auch der Zugang zu amtlichen Dokumenten eingeschränkt. Damit haben sich unsere Kolleg_innen aus dem Bereich der Informationsfreiheit befasst. Näheres erfahren Sie in unserem Tätigkeitsbericht zur Informationsfreiheit 2024/2025 unter https://www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht/

zeichnungen gelöscht werden, wenn sie nicht mehr für die Öffentlichkeit verfügbar sind. Denn der Zweck der Satzungsbefugnis aus den o.g. Vorschriften der GemO und LKrO ist die Ermöglichung der Veröffentlichung – wird dieser Zweck nicht mehr verfolgt, fehlt jeglicher Grund zu einer anderweitigen Verarbeitung.

3. Technische und organisatorische Schutzmaßnahmen („TOM“)

In der Satzung können auch die technischen und organisatorischen Schutzmaßnahmen geregelt werden. Dass angemessene TOM getroffen werden müssen, ergibt sich allerdings bereits direkt aus der DS-GVO, (insbesondere Art. 5 Abs.1 Buchst. f), 24, 32 DS-GVO. Wir empfehlen hier z.B.:

- Klar erkennbare Bereiche im Sitzungsraum, die erfasst, bzw. nicht erfasst werden
- Klare Regeln darüber, wann die Aufzeichnung / das Streaming beginnt
- Einblendungen auf dem veröffentlichten Video mit Hinweisen zu den Zwecken und der Grenzen der Zulässigkeit der Weiterverbreitung
- Veröffentlichung der Aufzeichnungen in einem für die verantwortliche Stelle technisch kontrollierbaren Rahmen, d.h. in einer Umgebung, über deren Einrichtung und Funktionen die verantwortliche Stelle entscheiden kann, also insbesondere nicht die Nutzung einer Plattform, die sich Rechte zur Weiterverarbeitung bereits in den AGB einräumt oder den Download ermöglicht / erleichtert (s.dazu auch unsere Handreichung zur Einbindung von Videos in eigene Webseiten)

Mit den Änderungen in der GemO und LKrO kann ein Aufzeichnen und Streamen von kommunalen Gremiensitzungen nun auf eine Satzung gestützt werden. Wir empfehlen, in der Satzung transparente und klare Regelungen zu treffen und das Interesse an Bürgerbeteiligung und Transparenz sorgfältig mit den Rechten der betroffenen Personen abzuwägen.

3.5. Novellierung des Landeskrankenhausgesetzes hinsichtlich der Forschungsregelungen

Art. 57 Abs.1 Buchst. c) DS-GVO

Die Landesregierung hat eine Änderung des Landeskrankenhausgesetzes Baden-Württemberg (LKHG BW) hinsichtlich der Regelung der Datenverarbeitung zu Forschungszwecken initiiert (s.die in den Landtag eingebrachte Fassung in LT-Drs.17/9482 und das vom Landtag beschlossene Gesetz in GBl. 2025 Nr. 121). Wir haben uns bei der Ausarbeitung der Regelungen intensiv eingebracht. Auf Initiative aus der Mitte des Landtags sind zudem wesentliche neue Gesichtspunkte aufgenommen worden.

Wir gehen davon aus, dass wir unsere Beratungsleistungen im Zusammenhang mit dem LKHG BW auch im kommenden Jahr fortsetzen werden und bieten an, auch die Evaluierung der Gesetzesänderung fachlich zu begleiten. Die Vielfalt der Forschungsfragen, die Bedeutung der Gesundheitsforschung für die Gesundheitsvorsorge und -versorgung einschließlich damit verbundener (volks-)wirtschaftlicher Interessen, die europarechtlichen Vorgaben aus der Verordnung zum Europäischen Gesundheitsdatenraum (European Health Data Space – EHDS) und weitere intensive gesetzgeberischen Aktivitäten lassen zusätzlich auch in Zukunft einen hohen Beratungsbedarf bei den unserer Aufsicht unterliegenden Stellen erwarten.

Das Thema der Verarbeitung personenbezogener Daten einschließlich von Daten aus der Gesundheitsversorgung zu Forschungszwecken ist schon länger eines, das Politik, Wirtschaft, Forscherinnen und Forscher sowie die Datenschutzaufsichtsbehörden intensiv beschäftigt.

Dabei möchten die Forschenden und die Wirtschaft insbesondere die bei verschiedenen Stellen vorhandenen Daten nutzen können, um aus ihnen neue wissenschaftliche Erkenntnisse zu gewinnen. Im Bereich der Gesundheitsforschung geht es hier insbesondere

um so erstrebenswerte Ziele wie die Verbesserung der Vorsorge vor Krankheiten und der Behandlung von Krankheiten, letzteres sowohl mit Blick auf die Erhöhung von Heilungschancen und Linderung von Beschwerden als auch mit Blick auf die Verbesserung der Versorgung und die Verringerung des Versorgungsaufwands. Auf der anderen Seite ist bei der Schaffung von Regelungen zur Verarbeitung von Daten aus der Gesundheitsversorgung zu Forschungszwecken aber zu sehen, dass es sich bei den Daten regelmäßig um hochsensible Informationen handelt, die – zum Teil unter mehreren Aspekten – unter den besonderen Schutz von Art. 9 DS-GVO fallen, soweit es sich etwa um Gesundheitsdaten oder genetische Daten handelt. Auch Daten zum Sexualleben oder zu religiösen Überzeugungen können im Rahmen der Gesundheitsversorgung anfallen. Die Daten aus der Gesundheitsversorgung, die zusätzlich zum datenschutzrechtlichen Schutzregime in der Regel auch durch berufsrechtliche Verschwiegenheitsverpflichtungen geschützt sind, benötigen daher eine besonders vertrauliche Behandlung, was bei der

Infokasten

Die Datenschutzkonferenz (DSK) hat sich kontinuierlich mit dem Thema „Forschung mit Gesundheitsdaten“ befasst:

Zu den Arbeiten der DSK zur Auslegung und Anwendung des GDNG siehe Beitrag in diesem Tätigkeitsbericht in Kap. 3.6.

Orientierungshilfe „Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken“ von September 2025: https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen.pdf sowie Anlage hierzu „Empfehlungen für Informationspflichten bei Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken“, ebenfalls von September 2025: https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen_Anlage.pdf

Beschluss „DS-GVO privilegiert wissenschaftliche Forschung - Positionspapier zum Begriff ‚wissenschaftliche Forschungszwecke‘“, vom 11. September 2024: https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf

Beschluss „Positionspapier - Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken“, vom 15. Mai 2024: https://www.datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf

Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“, vom 23. November 2023: https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

Entschließung „Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register“, vom 22./23. November 2023: https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

Petersberger Erklärung, vom 24.11.2022: https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Weiterverarbeitung auch zu Forschungszwecken zu berücksichtigen ist. Denn sowohl die Gesundheitsversorgung als auch die Gesundheitsforschung sind auf das Vertrauen von Patientinnen und Patienten sowie von Probantinnen und Probanten angewiesen.

Beteiligung im Vorfeld des Anhörungsverfahrens zur Forschung mit Gesundheitsdaten

In Baden-Württemberg begleiten wir die Thematik schon seit Längerem, u. a. durch die Beratung in verschiedenen Forschungsprojekten, durch die Beteiligung an zahlreichen Veranstaltungen zum Thema (auch in unseren KI-Wochen), aber auch durch unsere Vernetzung beispielsweise im Forum Gesundheitsstandort Baden-Württemberg.

Der Thematik wenden sich auch die Gesetzgeber des Bundes und der Länder verstärkt zu. Dazu kommen künftig mit dem EHDS auch unionsrechtlich gesundheitsdatenspezifische Vorgaben. Im Berichtszeitraum haben wir uns nicht nur mit dem seit 2024 in Kraft befindlichen Gesundheitsdatennutzungsgesetz (GDNG) des Bundes intensiv befasst. Auch die Landesregierung kam auf uns zu, um die Regelungen des Landeskrankenhausgesetzes zu novellieren, die die Verarbeitung personenbezogener Daten zu Forschungszwecken betreffen.

Gemeinwohlorientierung und Patientenversorgung im Fokus

Dabei verfolgte die Landesregierung das politische Ziel, die Verarbeitung der in den Krankenhäusern anfallen-

Infokasten

„Gesundheitsdatennutzung – Forschung, Innovation, klinische Versorgung und Ethik“, Vortrag und Diskussion, Philipp Kellmeyer, KI-Woche 2024 des LfDI: https://tube.bawü.social/w/vCC6m2Jqne5NiQvUEjt5fk?start=1s

Positionspapier der DSK zum Begriff „wissenschaftliche Forschungszwecke“ mit dem Titel „DS-GVO privilegiert wissenschaftliche Forschung“ vom 11. September 2024, S. 3 f. unter V.: https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf

„Forschung und Gesundheitsdaten“, LfDI BW, 40. Tätigkeitsbericht Datenschutz, S. 16ff.: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/03/TB_40_Datenschutz-2024_barrierefrei.pdf

„Gesundheitsdaten und Forschung – weiterhin ein großes Thema“, LfDI BW, 39. Tätigkeitsbericht Datenschutz, S. 92ff.: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf

„Beratung bei der Forschung“, LfDI BW, 38. Tätigkeitsbericht Datenschutz, S. 17ff.: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2023/02/TB_38_Datenschutz-2022_V1-.pdf

Ausführungen zum Forum Gesundheitsstandort BW:

LfDI BW, 39. Tätigkeitsbericht Datenschutz 2023, S. 96: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf

LfDI BW, 39. Tätigkeitsbericht Datenschutz 2022, S. 22f: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2023/02/TB_38_Datenschutz-2022_V1-.pdf

den Versorgungsdaten zu Zwecken dem Gemeinwohl dienender und mit der Versorgung zusammenhängender Forschungsthemen zu erleichtern und auf klarere gesetzliche Grundlagen zu stellen. Das Ziel der Klärung der Rechtsgrundlagen war u. a. schon deswegen nachvollziehbar, weil bereits seit einigen Jahren im Landeskrankenhausgesetz ein Widerspruch bestand. In § 43 Abs. 3 des Landeskrankenhausgesetzes in der bis zum 2. Dezember 2025 geltenden Fassung (im Folgenden: „LKHG a. F.“) war nämlich bestimmt, dass die Vorschriften des siebten, den Datenschutz betreffenden Abschnittes des Gesetzes nicht gelten würden für die Datenverarbeitung für Zwecke wissenschaftlicher Lehre oder Forschung. Dennoch fand sich sodann in diesem Abschnitt des Gesetzes in § 46 Abs. 1 Nummer 2a LKHG a. F. eine Regelung explizit über die Übermittlung personenbezogener zu Forschungszwecken. Auch das Anliegen, die Verwendung von Daten zu dem Gemeinwohl dienenden Forschungszwecken möglichst praktikabel auszugestalten, ist für uns – auch vor dem Hintergrund der Wertungen der Datenschutz-Grundverordnung, die die Forschung zu Recht privilegiert – grundsätzlich nachvollziehbar.

Das gesetzgeberische Unterfangen war alles andere als einfach. Zu beachten waren zum einen die Vorgaben der Datenschutz-Grundverordnung. Diese verlangt insbesondere für jede Verarbeitung von besonderen Kategorien personenbezogener Daten nicht nur eine Befreiung vom Verarbeitungsverbot aus Art. 9 Abs. 1 DS-GVO nach Maßgabe von Art. 9 Abs. 2 bis 4 DS-GVO, sondern auch einen Rechtsgrund im Sinne von Art. 6 Abs. 1 DS-GVO. Dabei ist der für nicht-öffentliche forschende Stellen (bei Fehlen einer Einwilligung) einschlägige Rechtsgrund typischerweise die Wahrnehmung berechtigter Interessen gemäß Art. 6 Abs. 1 Buchst. f) DS-GVO, und dieser Rechtsgrund ist für den nationalen Gesetzgeber nicht disponibel. Krankenhäuser können unterschiedliche Rechtsformen haben, Unikliniken sind öffentliche Stellen, andere Krankenhäuser sind zum Teil Wettbewerbsunternehmen der öffentlichen Hand, sodass diese andere rechtliche Regelungen zu beachten haben. Zudem hat der Bundesgesetzgeber mit verschiedenen Bestimmungen in § 6 GDNG Regelungen zur Verarbeitung personenbezogener Daten zu Forschungszwecken getroffen, ohne dass vollkommen klar wäre, inwieweit hier eine Gesetzgebungskompetenz des Bundes und inwieweit eine solche der Länder besteht.

Schon deswegen ist es positiv hervorzuheben, dass das Sozialministerium im Rahmen der Erstellung des Gesetzesentwurfs unsere Behörde frühzeitig beteiligt und uns mehrfach Gelegenheit zur Erörterung der Kerninhalte des Änderungsgesetzes gegeben hat. Wir konnten so bereits im Vorfeld der eigentlichen Anhörung an mehreren Entwurfsfassungen der Gesetzesnovelle beratend mitwirken und nahm an diversen Besprechungsterminen mit dem federführenden Ressort teil. Zusätzlich gestalteten wir gemeinsam mit Vertreter_innen des Staatsministeriums, des Sozialministeriums, des Wissenschaftsministeriums, des Innenministeriums und des Wirtschaftsministeriums sowie der Forschung einen Workshop zur geplanten Gesetzesänderung. Es schlossen sich weitere Arbeitssitzungen mit dem Sozialministerium und Vertreterinnen und Vertretern aus Wissenschaft und Forschung an. Und noch im weiteren Verlauf des Gesetzgebungsverfahren hatten wir sowohl Gelegenheit zur schriftlichen Stellungnahme als auch zur Erörterung in Videokonferenzen mit mehreren der beteiligten Ministerien und Vertreter_innen der Forschung.

Stellungnahme im Anhörungsverfahren

Nach der Begründung des Gesetzentwurfs in LT-Drs. 17/9482, S. 7 ist die Landesregierung davon ausgegangen, dass die Nutzung von Gesundheitsdaten, die bei einer datenverarbeitenden Gesundheitseinrichtung zu Versorgungszwecken vorhanden sind, zu Forschungszwecken durch die betreffende Gesundheitseinrichtung selbst (zuweilen auch „Eigenforschung“ genannt) durch § 6 Abs. 1 GDNG abschließend geregelt werde. Die Novelle habe daher insoweit nur noch die „Weitergabe“ von personenbezogenen Daten zu regeln.

Der uns im Rahmen der Anhörung zuletzt vorgelegte Entwurf enthielt bereits viele positiv zu bewertende Aspekte: Hervorzuheben ist insoweit insbesondere, dass die Forschungsthemen bestimmt werden, zu denen die Daten sollen weiterverarbeitet werden können, und mit der ursprünglichen Zweckbestimmung der Daten noch in einem nachvollziehbaren Zusammenhang stehen: In § 48 LKHG (neu), der die wesentlichen neuen Regelungen enthält, wird ausdrücklich bestimmt, dass es sich um eine Weiterverarbeitung zur „medizinischen, rehabilitativen oder pflegerische Forschung“ handeln muss. Bereits in der Überschrift kommt zudem zum Ausdruck, dass es sich um „gemeinwohlorientierte“ Forschung handeln muss. Das hebt den erforderlichen Gemeinwohlbezug der Forschung, der für die Privilegierung nach der Datenschutz-Grundverordnung vorauszusetzen ist zu Recht noch einmal deutlich hervor (s. Positionspaper der DSK zum Begriff „wissenschaftliche Forschungszwecke“ vom

11. September 2024, S. 3 f.). Zu begrüßen ist auch die in der Regelung normierte Anforderung, dass „das Forschungsinteresse die schutzwürdigen Belange der betroffenen Person überwiegt". Auf diese Weise wird nicht nur die Sensibilität der zu verarbeiteten Daten berücksichtigt, sondern sichergestellt, dass zugunsten nicht-öffentlicher Stellen in aller Regel auch die Verarbeitungsbefugnis aus Art. 6 Abs. 1 Buchst. f) DS-GVO vorliegt, so dass hier eine Entscheidung, inwieweit die Regelung im Krankenhausgesetz für diese selbst einen Rechtsgrund im Sinne von Art. 6 DS-GVO schaffen kann, für die Praxis weitgehend dahinstehen kann (vgl. hierzu die Ausführungen LT-Drs. 17/9482, S. 8).

Schließlich sah der Novellierungsentwurf, der insoweit unverändert vom Landtag beschlossen wurde, in § 48 Abs. 2 und 3 LKHG eine Reihe konkreter und nachvollziehbarer technischer und organisatorischer Schutzmaßnahmen und sowie von Garantien vor, um die Anforderungen aus Art. 9 Abs. 2 Buchst. j) sowie Art. 89 Abs. 1 DS-GVO zu erfüllen. Fraglich bleibt allerdings, inwieweit es gelingen kann, die Einhaltung dieser Maßnahmen und Garantien auch aufsichtsrechtlich durchzusetzen. Unsere Hinweise darauf, dass es hier Verbesserungsbedarf gibt, sind im Gesetzgebungsverfahren leider nicht angenommen worden. Im Rahmen der vom Landtag bei der Verabschiedung des Gesetzes beschlossenen Evaluation (s. Plenarprotokoll 17/134, S. 8128) wird auch diese Thematik erneut zu betrachten sein.

Intensive Beratung zum Einbezug genetischer Daten zu Forschungszwecken

Besonders intensiv erörtert wurde von Seiten unserer Behörde im Rahmen der Beratung zur Entwurfsfassung die Regelung zur Verarbeitung genetischer Daten zu den genannten Forschungszwecken. Genetische Daten (zur Definition s. Art. 14 Nummer 13 DS-GVO) sind typischerweise sehr eng mit der Persönlichkeit der betroffenen Person verknüpft und haften ihr ein Leben lang an. Sie können ein hohes prädiktives Potenzial mit Blick auf die Person selbst und biologische Verwandte enthalten und bergen daher ein hohes Diskriminierungs- und Stigmatisierungsrisiko. Eine wirksame Anonymisierung ist bei genetischen Daten zudem regelmäßig nicht möglich. Der Bundesgesetzgeber hat daher schon im Gendiagnostikgesetz (GenDG) u. a. vorgesehen, dass eine genetische Untersuchung oder Analyse nur vorgenommen und eine dafür erforderliche genetische Probe nur gewonnen werden darf, wenn die betroffene Person in die Untersuchung und die Gewinnung der dafür erforderlichen genetischen Probe ausdrücklich und schriftlich gegenüber der verantwortlichen ärztlichen Person eingewilligt hat (vgl. § 8 GenDG). Die DSK hat dementsprechend zuletzt in ihrem Positionspapier „Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken" vom 15. Mai 2024 zu Recht ausgeführt, dass der Umgang mit genetischen Daten qualifizierten datenschutzrechtlichen Regeln unterliegen muss, die die Rechte und Freiheiten der betroffenen Person in ausreichendem Maße wahren. Für die datenschutzkonforme Verarbeitung genetischer Daten bedarf es daher grundsätzlich der ausdrücklichen Einwilligung der betroffenen Personen.

Von diesem Grundsatz darf es mit Blick auf die individuelle Rechtsausübung der infomationellen Selbstbestimmung nur enge Ausnahmen geben. In der Diskussion mit Forschenden konnten wir dabei als eine mögliche Ausnahme herausarbeiten, dass nach der Geburt erworbene – wie insbesondere durch Tumore veränderte – genetische Informationen zum einen für die medizinische Forschung von erheblicher Bedeutung, zum anderen aber auch weniger eng mit der betroffenen Person selbst und deren Verwandtschaft verbunden sind, so dass es hier vertretbar erscheint, unter den übrigen im Gesetzentwurf vorgesehenen Kautelen eine Verarbeitung zu den dort vorgesehenen Forschungszwecken ausnahmsweise auch ohne Einwilligung zuzulassen (vgl. § 48 Abs. 1 Satz 1 Nummer 1 LKHG – neu).

Aus Sicht der Forschenden wäre allerdings alleine mit dieser Ausnahme dem Forschungsinteresse nicht hinreichend Genüge getan. Sie machten insbesondere geltend, dass vielmals die Untersuchung einzelner Sequenzvarianten für die medizinische Forschung von großem Wert sei, dass aber zugleich bei Betrachtung nur einzelner Varianten das Identifikationsrisiko gering sei. Unter einzelnen Sequenzvarianten seien dabei spezifische, abgegrenzte genetische Veränderungen an einer bestimmten Position im Genom zu verstehen (wie dies nunmehr in der Gesetzesbegründung erläutert wird). Hier war jedoch das Risiko gesetzgeberisch einzugrenzen, dass gleichwohl infolge der Einzigartigkeit einer genetischen Variante oder der Kombination von mehreren Varianten jedenfalls bei Hinzutreten weiterer Informationen eine Identifikation der betroffenen Person möglich sein könnte. Aus Sicht des Datenschutzes wäre es insoweit angesichts der hohen Sensibilität der (hier ererbten) genetischen Daten zum Schutz vor dem Identifikationsrisiko wünschenswert gewesen zu bestimmen, dass die Information aus den

Varianten bzw. den Variantenkombinationen dann nicht übermittelt werden dürfen, wenn sie unter Bezugnahme auf die Stichprobenart und die Menge des die Voraussetzungen der Stichprobe erfüllenden Teils der Weltbevölkerung voraussichtlich einzigartig ist. Die Landesregierung befürchtete jedoch, dass dadurch der Übermittlung genetischer Daten zu Forschungszwecken zu enge Grenzen gesetzt würden. Deswegen erachtete sie es in Abwägung mit dem Ziel der Förderung des wissenschaftlichen Erkenntnisinteresses für ausreichend, die Übermittlung nur dann auszuschließen, wenn die zur Übermittlung anstehenden Sequenzvarianten in ihrer Kombination nach dem Stand der Wissenschaft voraussichtlich einzigartig in der Weltbevölkerung sind, ohne Rücksicht auf die weiter eingrenzenden Eigenschaften der verwendeten Stichprobe. Auch insoweit wird es hilfreich sein, der Frage, ob dies zur Verringerung des Identifikationsrisikos ausreichend ist, im Rahmen der vom Landtag beschlossenen Evaluation zu überprüfen.

Voraussetzungsloses Widerspruchsrecht

Besonderen Wert legten wir zuletzt im Rahmen unserer Stellungnahme darauf, dass der Gesetzgeber den betroffenen Personen, auch wenn die Übermittlung der personenbezogenen Daten auf eine einwilligungsunabhängige gesetzliche Befugnis gestützt werden soll, eine praktikable Möglichkeit der Einflussnahme auf die Verwendung ihrer sensiblen Daten durch Einräumung eines voraussetzungslosen Widerspruchsrechts schafft. Dieses ist in besonderem Maße geeignet, das Vertrauen in das Gesundheitswesen und die Akzeptanz der gesetzlichen Regelung zu Forschungszwecken zu fördern. Insoweit betonten wir, dass das Gesundheitswesen primär die Aufgabe hat, (im Rahmen der Finanzierbarkeit) allen Menschen diskriminierungsfrei den Zugang zu der für sie notwendigen Versorgung zu ermöglichen. Für die Inanspruchnahme einer Behandlung der Gesundheitsversorgung ist aber ein besonderes Vertrauen der Patientinnen und Patienten erforderlich; hierzu gehört es, dass sie grundsätzlich davon ausgehen können sollten, dass die den Gesundheitsversorgern anvertrauten Daten auch vertraulich behandelt werden. Der Zugang zur Gesundheitsversorgung muss auch solchen Personen angstfrei und unbelastet möglich sein, die sich davor sorgen, dass ihre Gesundheitsdaten außerhalb der Behandlungskontextes Personen oder Einrichtungen zu Forschungszwecken überlassen werden. Dabei ist auch zu berücksichtigen, dass selbst bei Pseudonymisierung und Ergreifung von weiteren technischen und organisatorischen Maßnahmen ein Offenbarwerden der personenbezogenen Daten gegenüber Unbefugten tatsächlich nicht vollkommen ausgeschlossen werden kann. Wir verwiesen weiterhin darauf, dass der Gesetzgeber mit der Einräumung eines voraussetzungslosen Widerspruchsrechts auch eine Harmonisierung herstellt u. a. mit den Regelungen der Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum, nach der grundsätzlich ein Recht zum voraussetzungslosen Widerspruch gegen eine Sekundärnutzung der Gesundheitsdaten vorzusehen ist (s. Art. 71 und Erwägungsgrund 54; vgl. ferner auch § 363 Abs. 5 des Fünften Buchs des Sozialgesetzbuchs). Ein voraussetzungsloses Widerspruchsrecht ist außerdem unseres Erachtens sowohl für die betroffenen Personen als auch für die forschenden Stellen unbürokratischer als das ansonsten ohnehin greifende Widerspruchsrecht aus Art. 21 Abs. 1 und 6 DS-GVO, bei dem die Patientinnen und Patienten dartun (und die übermittelnden Krankenhäuser ggf. prüfen) müssen, warum sich aus ihrer besonderen Situation Gründe gegen die Weiterverarbeitung zu Forschungszwecken ergeben.

Die Auswirkungen eines solchen Widerspruchsrechts auf die Forschung schätzten wir als wenig einschränkend ein. Denn die meisten Patientinnen und Patienten haben Verständnis für die Notwendigkeit von Forschung in den hier relevanten Forschungsfeldern und sind bereit diese zu unterstützen. Die Quote derjenigen, die tatsächlich von dem Widerspruchsrecht Gebrauch machen werden, wird daher voraussichtlich – jedenfalls so lange die Patientinnen und Patienten den Eindruck haben, dass mit ihren Daten im Allgemeinen sorgfältig verfahren wird, – in einem so geringen Bereich liegen, dass die Stichprobengröße für die Forschung nicht relevant beeinträchtigt wird.

Erweiterung des Anwendungsbereiches durch Ausweitung der Zwecke

Der Landtag hat inzwischen über die Gesetzesinitiative der Landesregierung entschieden und den Entwurf in der Sitzung vom 12. November 2025 (s. das oben erwähnte Plenarprotokoll) weitgehend angenommen. Auf Basis einer Beschlussempfehlung des Ausschusses für Soziales, Gesundheit und Integration wurde eine wesentliche Erweiterung des Anwendungsbereichs von § 48 LKHG-neu beschlossen. Nach dieser Änderung soll die Neuregelung nicht nur für die bei der Gesetzesinitiative allein in Rede stehende Übermittlung zu Forschungszwecken erfassen, sondern insbesondere auch

eine „Weitergabe von personenbezogenen Daten zur Qualitätssicherung und zur Förderung der Patientensicherheit“. Die auf diese Weise geschaffene Regelung von Datenverarbeitungen zu anderen Zwecken ist indes in mehrfacher Hinsicht problematisch. Zum einen ist bei einer solchen Regelung zu bedenken, dass für die genannten anderen Verarbeitungszwecke nicht die ausschließlich für die Verarbeitung zu Zwecken der wissenschaftlichen Forschung geltende Privilegierung der DS-GVO einschlägig ist. Außerdem erachten wir die Zweckbestimmungen „Patientensicherheit“ und „Qualitätssicherung“ in dieser Form für nicht hinreichend bestimmt, um den Rechtsanwendenden und Rechtsunterworfenen eine hinreichend sichere Prognose zu ermöglichen, welche Datenverarbeitungen hiervon umfasst sein sollen und welche nicht.

Es ist zu begrüßen, dass das Gesetz nach dem Willen des Landtags ein Jahr nach seinem In-Kraft-Treten evaluiert werden soll. Dabei wird zudem Gelegenheit bestehen, das Gesetz noch in Bezug auf weitere Punkte (wie beispielsweise die Verwendung unterschiedlicher Begrifflichkeiten – „Übermittlung“ in §§ 46 und 47 LKHG versus „Weitergabe“ in § 48 LKHG, die Frage der Abgrenzung zwischen § 46 Abs.1 Buchst. 2a LKHG zur neugeschaffenen Regelung in § 48 LKHG, die unnötig und damit weitere Fragen aufwerfende Formulierung „ohne Einwilligung der betroffenen Person“ in § 48 Abs.1 LKHG u.a. m.) zu präzisieren und insbesondere auch die Regelungen der Datenverarbeitung zur Qualitätssicherung insgesamt (auch in § 46 Abs.1 Nummer 2 LKHG), zu denen wir in anderem Zusammenhang bereits mit dem Sozialministerium im Gespräch waren, zu verbessern.

Infokasten

Positionspapier der DSK zum Begriff „wissenschaftliche Forschungszwecke“ mit dem Titel „DS-GVO privilegiert wissenschaftliche Forschung“, vom 11. September 2024, S.3 f. unter V.: https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf

3.6. Exkurs: Gesundheitsdatennutzungsgesetz

Im Kapitel zu Europa sprechen wir unter anderem über unser Engagement im Rahmen von europäischen Regelungen und darüber, wie wir Leitlinien erarbeiten, damit in Europa das geltende Recht einheitlich angewendet wird. In diesem Kapitel sprechen wir über unsere Beteiligung auf Landesebene. Hier nun möchten wir in einem Exkurs über unsere Arbeit in der Datenschutzkonferenz (DSK) zur Schaffung einheitlicher Anwendungsmaßstäbe berichten, nämlich zum nationalen Gesundheitsdatennutzungsgesetz (GDNG). Das Gesetz steht mit der Thematik der zuvor erwähnten Novelle des Landeskrankenhausgesetzes in einem engen Zusammenhang. Denn auch im GDNG sind insbesondere Regelungen zur Forschung mit Gesundheitsdaten enthalten. Die verschiedenen Regelungsebenen sind (insbesondere für Forschende und die Gesundheitseinrichtungen, aber auch für betroffene Personen) kompliziert genug; um so wichtiger ist es für uns zu erreichen, dass das neue Bundesrecht durch die Aufsichtsbehörden möglichst einheitlich angewandt wird. Deswegen haben wir uns besonders eingebracht in eine Arbeitsgruppe, die auf ein gemeinsames Verständnis und eine abgestimmte Handhabung des GDNG ausgerichtet ist. Unser Ziel ist es, möglichst wirksam dabei zu helfen, dass Forschung und Datenschutz in Einklang gebracht werden.

Gesundheitsdaten für die Forschung

Im März 2024 trat das GDNG in Kraft. Mit diesem hat der Gesetzgeber u.a. eine neue Rechtsgrundlage für die Verarbeitung von Gesundheitsdaten durch „öffentlich geförderte Zusammenschlüsse von datenverarbeitenden Gesundheitseinrichtungen“ geschaffen (Näheres siehe unter 1.). Ein weiteres Ziel des Gesetzes ist es, für gemeinwohlorientierte Forschungsvorhaben „die Verfahren zur Abstimmung mit den Datenschutzaufsichtsbehörden zu vereinfachen und gleichzeitig den Gesundheitsdatenschutz zu stärken“ (Näheres siehe unter 2.).

Die Umsetzung der neuen Regelungen führt für die vom Gesundheitsdatennutzungsgesetz adressierten Akteure wie z. B. Arztpraxen, Krankenhäuser oder Apotheken zu einer Vielzahl von Fragen. Diese stellen sich auch für die Datenschutzaufsichtsbehörden, und aus diesem Grund hat die – schon früher zu Fragen des Datenschutzes im Bereich der medizinischen Forschung von der Datenschutzkonferenz eingerichtete – Taskforce

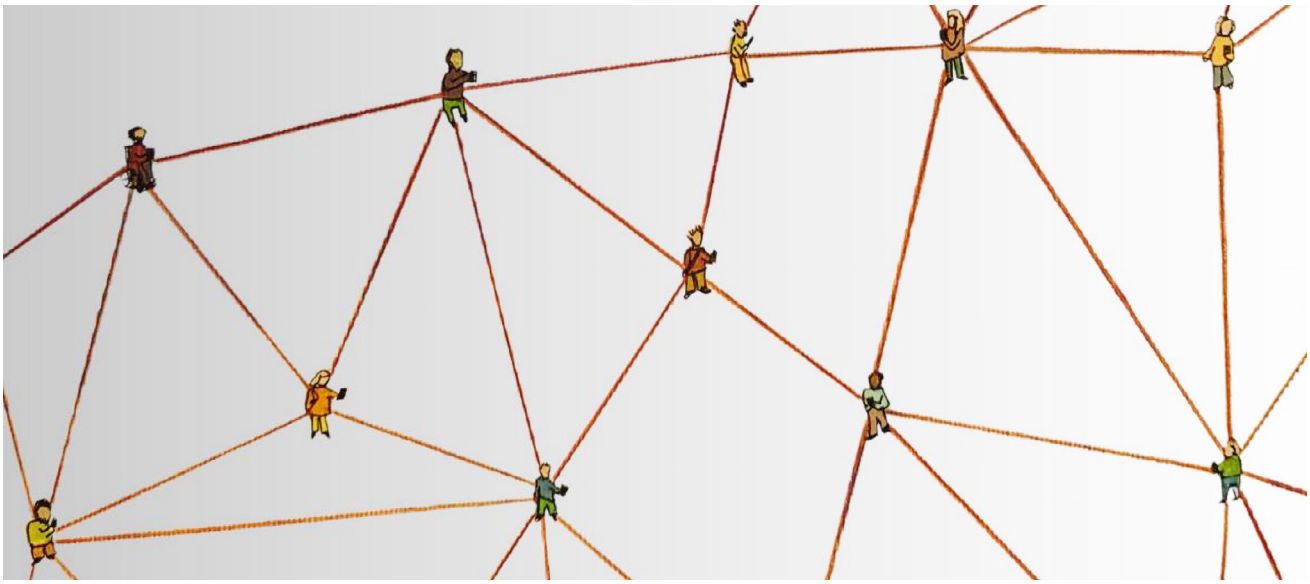


Bild: Jamillah Knowles & Reset.Tech Australia / https://betterimagesofai.org / https://au.reset.tech/ / https://creativecommons.org/licenses/by/4.0/

Forschungsdaten kurz nach Inkrafttreten des Gesetzes die Arbeitsgruppe Gesundheitsdatennutzungsgesetz (im Folgenden: AG GDNG) eingesetzt, deren Vorsitz Baden-Württemberg übernommen hat. Die inzwischen seit Juni 2024 bestehende Arbeitsgruppe hat sich bislang u.a. mit den folgenden Themenfeldern befasst:

1. Einheitliches Antragsformular und Musterbescheid

Nach der neuen Rechtslage dürfen öffentlich geförderte Zusammenschlüsse von datenverarbeitenden Gesundheitseinrichtungen Gesundheitsdaten zu Zwecken der Qualitätssicherung und Förderung der Patientensicherheit, zur medizinischen, rehabilitativen und pflegerischen Forschung und zu statistischen Zwecken gemeinsam verarbeiten, ohne dass hierfür eine Einwilligung der betroffenen Personen erforderlich ist (vgl. § 6 Abs. 3 Satz 4 GDNG).

Voraussetzung ist insbesondere, dass die Interessen des datenschutzrechtlich Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Des Weiteren ist eine Zustimmung der zuständigen Datenschutzaufsichtsbehörde erforderlich.

Die AG GDNG hat zur Einholung der jeweiligen Zustimmung ein einheitliches Antragsformular für die antragstellenden Gesundheitseinrichtungen erarbeitet. Aus diesem ergibt sich, welche Informationen und Dokumente benötigt werden, was die Antragstellung erleichtert. Das Antragsformular kann auf der Internetseite des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (der zusammen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Taskforce Forschungsdaten leitet) unter https://datenschutz.hessen.de/service/antrag-auf-zustimmung-nach-ss-6-abs-3-s-4-nr-4-gdng abgerufen werden.

Weiter hat die Arbeitsgruppe einen Musterbescheid für eine Zustimmung zur gemeinsamen Nutzung und Verarbeitung der Daten durch die jeweilige Datenschutzaufsichtsbehörde erstellt.

2. Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden

Das neue Gesetz trifft Regelungen zur Datenschutzaufsicht bei länderübergreifenden Vorhaben der Versorgungs- oder Gesundheitsforschung (vgl. § 5 GDNG). Bei gemeinsamen Vorhaben mehrerer verantwortlicher Stellen, die der Datenschutzaufsicht unterschiedlicher staatlicher Aufsichtsbehörden unterliegen, kann unter bestimmten Voraussetzungen einer Aufsichtsbehörde die Federführung oder die alleinige Zuständigkeit übertragen werden.

Die AG GDNG hat hier eine Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG erarbeitet, welche bei der 110.

Datenschutzkonferenz verabschiedet wurde. Dieses Papier unterstützt einerseits die Arbeit der Aufsichtsbehörden der Länder und des Bundes, stellt zugleich aber auch eine Auslegungshilfe für die forschenden Stellen dar.

3. Versorgungsdaten, Sicherheit, Forschung

Die Arbeit der Arbeitsgruppe wird noch fortgesetzt. Derzeit wird insbesondere ein einheitlichen Verständnis in Bezug auf Auslegungsfragen zu § 6 GDNG erarbeitet.

Die Datenschutzkonferenz und ihre Gremien haben sich auch im Berichtszeitraum das Ziel gesetzt, die datenschutzkonforme Nutzung personenbezogener Daten zu Forschungszwecken zu unterstützen, und diesbezüglich wichtige Schritte unternommen.

Infokasten

Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG): https://dserver.bundestag.de/btd/20/090/2009046.pdf

Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz – GDNG): https://www.gesetze-im-internet.de/gdng/BJNR0660B0024.html

Datenschutzkonferenz macht Reformvorschläge für die Datenschutz-Grundverordnung, Pressemitteilung vom 12. Dezember 2025: https://datenschutzkonferenz-online.de/media/pm/DSK_PM_110_DSK.pdf

DSK-Orientierungshilfe zur Zusammenarbeitmehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG, Dezember 2025: https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_Zusammenarbeit_mehrerer_Aufsichtsbehoerden_GDNG.pdf

3.7. Das neue Schulgesetz: gläserne Schulkarrieren?

Art. 57 Abs.1 Buchst. c) DS-GVO

Wir betrachten bei der datenschutzrechtlichen Bewertung von Vorschriften über die Verarbeitung personenbezogener Daten insbesondere, inwieweit die vorgesehene Verarbeitung mit Blick auf den damit verfolgten Zweck und auf die Intensität des damit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung geeignet, erforderlich und verhältnismäßig ist. Wir berücksichtigen auch, ob eine Vorschrift im Ergebnis missbräuchliche Datenverarbeitungen erleichtern könnte.

Im vergangenen Jahr wurde das Schulgesetz durch das Gesetz zur Änderung schulgesetzlicher Regelungen (LT-Drs.17/10033, GBl. 2025, Nr. 148) in vielfacher Hinsicht geändert. Bei der Ausarbeitung des Entwurfs (abgedruckt in LT-Drs 17/9653) hatte uns das Kultusministerium beteiligt. Viele unserer Hinweise wurden im Gesetzentwurf leider nicht berücksichtigt. Unsere folgenden Ausführungen beziehen sich ausschließlich auf den Gesetzentwurf (auch soweit wir zur besseren Orientierung eine Vorschrift des geänderten Schulgesetzes und nicht des Gesetzentwurfs nennen).

Durch das neue Schulgesetz sollen jeder Schülerin und jedem Schüler eine individuelle Identifikationsnummer zugeordnet werden, die für ihre oder seine gesamte schulische Laufbahn Gültigkeit behält (vgl. § 113a Abs. 3 Satz 1 des Schulgesetzes in der neuen Fassung). Auf diese Weise sollen vielfältige Informationen über die Schulkarriere jeder Schülerin und jedes Schülers leichter abrufbar sein.

Dabei sah der ursprüngliche Entwurf weitgehend undifferenziert ein nur über zahlreiche Regelungsverweise angedeutetes, letztlich aber kaum bestimmtes Zweckkonglomerat vor, dem die zentrale Erfassung und Weiterverarbeitung einer ebenfalls wenig umrissenen Menge von personenbezogenen Daten zu jeder Schülerin und jedem Schüler dienen sollte. Dies haben wir in unseren Stellungnahmen unter Hinweis insbesondere

auf die Verarbeitungsgrundsätze aus Art. 5 DS-GVO kritisiert. Wir haben dort u.a. ausgeführt, dass personenbezogene Daten nur für festgelegte und eindeutige legitime Zwecke erhoben werden dürfen (Art. 5 Abs.1 Buchst. c) DS-GVO) und dass bei einer Regelung, die eine Rechtsgrundlage für eine Datenverarbeitung im öffentlichen Interesse darstellen soll, in der Regel der jeweilige Zweck der Datenverarbeitung in der Norm selbst festgelegt sein muss (Art. 6 Abs.3 Satz 2 DS-GVO). Zudem haben wir darauf hingewiesen, dass personenbezogene Daten nur insoweit verarbeitet werden dürfen, als dies dem Zweck angemessen ist und die Daten erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden (Art. 5 Abs.1 Buchst. c) DS-GVO). Das Kultusministerium hat daraufhin den Entwurf etwas überarbeitet und in der neueren Version die Zwecke etwas näher zu bestimmen versucht (vgl. § 113a SchG-E in der in LT-Drs 17/9653 abgedruckten Fassung).

Infokasten

Der Gesetzentwurf der Landesregierung - Gesetz zur Änderung schulgesetzlicher Regelungen: LT-Drs.17 / 9653, vom 14. Oktober 2025: https://www.landtag-bw.de/resource/blob/600082/174986bcabb99b6785f4ee-ba814330fc/17_9653_D.pdf

Der Gesetzesbeschluss des Landtags - Gesetz zur Änderung schulgesetzlicher Regelungen: LT-Drs.17 / 10033, ausgegeben: 12. Dezember 2025: https://www.landtag-bw.de/resource/blob/610376/638630c437790d949462bd33c68def3d/17_10033_D.pdf

Läuft es mal nicht so gut? Sollte es die Möglichkeit geben, sich neu erfinden zu können? Oder soll man eine schlechte Phase immer mit sich tragen und damit konfrontiert werden?
Bild: Max Gruber / Better Images of AI / Clickworker 3d-printed / CC-BY 4.0

Die individuelle, die gesamte Schullaufbahn unverändert bleibende Identifikationsnummer für Schüler_innen soll zu den ganz unterschiedlichen Zwecken verwendet werden, Daten bei Schulwechsel zu übermitteln, schulübergreifende Verwaltungsaufgaben zu erledigen, Mehrfachbewerbungen festzustellen sowie „Bildungsverläufe nachzuvollziehen“(vgl. § 113a Absatz 3 Satz 2 SchG n. F.).

Wir können nicht nachvollziehen, dass dies nur mit dieser Nummer möglich sein soll. Insbesondere über die Schaffung solcher Bildungsverlaufsregister ist die Kultusministerkonferenz (KMK) schon seit vielen Jahren mit dem Arbeitskreis Bildung der Datenschutzkonferenz im Gespräch. Dabei hat der Arbeitskreis stets von der KMK gefordert, dass die Zwecke klar definiert weden und dargetan werden muss, dass zur Erreichung der Zwecke die jeweiligen Datenverarbeitungen erforderlich und angemessen sind. Eine solche Darlegung ist der KMK aus Sicht des Arbeitskreises Bildung bis heute nicht gelungen.

Im Grunde wird ein riesiger Datenspeicher für alle Schülerinnen und Schüler in Baden-Württemberg aufgebaut, der sensiblen Daten wie Leistungen, Noten und Zeugnisse speichert. Noch gravierender: Es sollen auch Gesundheitsdaten dazukommen.

Es ist nicht nachvollziehbar, warum diese Informationen unter einer einheitlichen Identifikationsnummer erfasst und – zu unterschiedlichen Zwecken – in einer zentralen Datei gespeichert werden müssen. Dies ist Vorratsdatenspeicherung sensibler Daten eines empfindlichen Personenkreises, der einen besonderen Schutz genießen sollte: Kinder und Jugendliche.

Die Schule und das Institut für Bildungsanalysen (IBBW) haben Zugriff auf diese Daten. Zwar soll ein Pseudonym verwendet werden, sodass nur die Schule den Namen zuordnen kann, nicht jedoch das IBBW oder Dritte. Aber in vielen Konstellationen wird durch geringes Zusatzwissen eine Identifizierung wahrscheinlich trotzdem möglich sein. Beispielswiese können etwa die Jahrgangsbesten einer Schule über Pressemeldungen identifiziert werden, oder Schüler_innen durch einen Schulwechsel oder eine ungewöhnliche Kursauswahl in der Oberstufe.

Weiterhin ist aus datenschutzrechtlicher Sicht nicht plausibel, warum die Oberstufe eines Gymnasiums noch auf Daten aus der Grundschule zugreifen sollte. Im Gesetz ist keine Begrenzung vorgesehen, wie lange diese Daten von der Schule in die Vergangenheit hinein eingesehen werden können. Eine Begründung hierfür fand sich nicht.

Die Übermittlung, auch sehr alter Daten, bei einem Schulwechsel erschwert Schüler_innen, die an ihrer alten Schule vielleicht Probleme hatten, einen Neuanfang an der neuen Schule. Wir haben dazu schon in der Vergangenheit Beschwerden von Eltern bekommen. Gerade Kindern und Jugendlichen muss es aber effektiv möglich bleiben, etwaige Fehler zu korrigieren und ggf. einen möglichst unbelasteten Neustart durchzuführen. Wenn ein junges Schulkind eine schlechte Phase in der Schule hatte, weil beispielsweise die Großmutter gestorben ist – warum sollte diese Trauer Teil der auswertbaren Bildungsbiografie werden?

Kapitel 4

Schulungs-zentrum und Veranstaltungen

4. Schulungszentrum und Veranstaltungen

In unserem hauseigenen Bildungszentrum bieten wir Schulungen an. Zudem organisieren wir Veranstaltungsreihen wie die KI-Woche, gehen auf Messen und Kongresse und suchen den direkten Austausch mit den Menschen.

4.1. Bildungszentrum BIDIB

Art. 57 Abs.1 Buchst. b), d) DS-GVO

Seit nun fünf Jahren gibt es das Bildungszentrum für Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB). Der Landtag hat es uns 2020 mit großem Weitblick ermöglicht, das bis heute in dieser Form bundesweit einzigartige Schulungsangebot in einer Aufsichtsbehörde vorhalten zu können. Das Angebot ist notwendiger denn je.

Die Auswirkungen deutschen und europäischen Rechtsakte im Bereich des Daten- und Digitalrechts auf die tägliche Praxis zeigt, dass viele Bürger_innen, Behörden und Unternehmen es als Herausforderung empfinden, den unterschiedlichen rechtlichen Anforderungen gerecht zu werden. Mit dem BIDIB als Schulungszentrum bieten wir zahlreiche praxisnahe und kostenfreie Schulungen für unterschiedliche Zielgruppen im Bereich Datenschutz und Informationsfreiheit an.

Das Bildungszentrum hat im vergangenen Jahr 71 Schulungen für Bürger_innen, Behörden, Unternehmen und Vereine angeboten. 3205 Menschen haben sich für die Schulungen angemeldet. Das sind insgesamt weniger Menschen als im Vorjahr, was insbesondere daran liegt, dass das Angebot von „Schule digital“ aufgrund von zum Jahresbeginn entfallenen kw-Stellen nicht mehr in dem bisherigen Umfang aufrechterhalten werden konnte. Wir arbeiten dennoch weiter intensiv daran, das Schulungsangebot des Bildungszentrums weiterzuentwickeln und auch künftig mit einem online verfügbaren Bildungsportal zu ergänzen.

Eine organisatorische Weiterentwicklung war die Angliederung des Bildungszentrums an die Abteilung für Informationsfreiheit in unserer Dienststelle. Die Zusammenführung wurde im Laufe des Jahres intensiv vorbereitet, organisatorisch begleitet und inhaltlich mitgedacht. Gegen Ende des Jahres konnte die Umstrukturierung vollzogen werden.

Neben den klassischen Schulungsformaten bei uns in der Dienststelle ergaben sich auch immer wieder Möglichkeiten unsere Schulungsinhalte und -formate bei externen Veranstaltungen zu präsentieren. So waren zahlreiche Referent_innen bei unterschiedlichen Kooperationsschulungsangeboten z. B. im Bildungsbereich beim Zentrum für Schulqualität und Lehrerbildung (ZSL) engagiert.

Insbesondere hervorzuheben ist dabei die zahlreiche Beteiligung von Referent_innen aus der Dienststelle an der jährlichen Datenschutzkonferenz des Berufsverbands der Datenschutzbeauftragten Deutschlands e.V. (BvD).

Die Herbstkonferenz und der Behördentag 2025 in München im Oktober 2025 fand bereits zum neunten Mal statt und wurde erneut in Kooperation mit dem Landesamt für Datenschutzaufsicht (BayLDA) und dem Bayerischen Landesbeauftragten für den Datenschutz (BayLfD), unserer Behörde und dem BvD durchgeführt. In diesem Jahr wurde unter dem Motto: „Erfolgreiche Datennutzung: Vertrauen durch Datenschutz“ das Verhältnis von Datennutzung und

Datenschutz thematisiert und in zahlreichen Vorträgen erörtert. Im beliebten Kurzformat „Die Aufsichtsbehörde beantwortet Ihre Fragen“ gab es die Möglichkeit, konkrete Problemstellungen aus der täglichen Arbeitspraxis direkt an die Landesbeauftragten zu adressieren.

Im kommenden Jahr 2026 fokussieren wir uns im BIDIB auf eine Erhöhung der Schulungsangebote zum Beispiel zum Thema Videoüberwachung und auf das digitale Bildungsportal. Wir freuen uns, erneut viele Menschen zu unseren Schulungen vor Ort begrüßen – und ihnen dabei auch unsere neue Dienststelle zeigen zu können.

4.2. Didacta 2025: ein Dialog zum Datenschutz in der Bildung

Art. 57 Abs.1 Buchst. b), c) DS-GVO

Die Didacta, die weltweit größte Bildungsmesse, fand dieses Jahr in Stuttgart statt. Auch wir waren dort – gemeinsam mit Aufsichtsbehörden aus weiteren Ländern – mit einem Stand vertreten, um den direkten Austausch mit Fachleuten, Lehrkräften, Schulleitungen, IT-Experten und anderen Interessierten zu fördern. Wir haben schätzungsweise mit über 1000 Menschen gesprochen, ihnen z. B. Informationen gegeben und kurze Beratungsgespräche geführt.

Die Präsenz der Datenschutz-Aufsichtsbehörden auf der Didacta hat sich in der Vergangenheit bewährt und leistet einen wichtigen Beitrag zur Sensibilisierung und Information im Bildungsbereich. Es ist eine einzigartige Gelegenheit, einen direkten Draht zu den Akteur_innen en vor Ort zu knüpfen und die Herausforderungen in der digitalen Bildung aus erster Hand kennenzulernen. Deswegen haben wir vom 11. bis zum 15. Februar 2025 mit einem gemeinsamen Stand mit anderen Aufsichtsbehörden an der Didacta teilgenommen. Besonders erfreulich war, dass uns eine hohe Anzahl an Besucher_innen aus Baden-Württemberg besuchte.

Infokasten

Datenschutz und Bildung – LfDI BW informiert auf der Bildungsmesse didacta: https://www.baden-wuerttemberg.datenschutz.de/datenschutz-und-bildung-lfdi-bw-informiert-auf-der-bildungsmesse-didacta/

Mit der Teilnahme an der Didacta kommt der Landesbeauftragte seiner Aufgaben gemäß Art. 57 Abs.1 Buchst. b) und c) der DS-GVO nach. Dazu gehört die datenschutzrechtliche Beratung im Bereich der Informations- und Kommunikationstechnologien und die Sensibilisierung für Datenschutzfragen. Die zunehmende Digitalisierung des Bildungswesens erfordert eine ständige Auseinandersetzung mit den damit verbundenen Risiken und die Entwicklung und Einhaltung geeigneter Schutzmaßnahmen. Die Didacta bietet für diese Sensibilisierungsaufgabe die ideale Plattform.

Die Möglichkeit, sich mit den Anwender_innen digitaler Lernmittel direkt auszutauschen, und die Chance, ihre Bedenken und Fragen besser zu verstehen, waren von großem Wert. Die Rückmeldungen der Besucherinnen und Besucher aus der Praxis der Schulen fließen in die weitere Arbeit des Landesbeauftragten ein. Viele Gespräche drehten sich um Themen wie die datenschutzkonforme Nutzung von Cloud-Diensten, die Einhaltung der Datenschutz-Anforderungen bei der Verarbeitung von Schülerdaten und die Möglichkeiten zur

Zusammen mit Kolleg_innen aus Berlin, Rheinland-Pfalz, Sachsen-Anhalt und Thüringen war der LfDI mit einem gemeinsamen Stand auf der Didacta 2025 präsent. Bild: LfDI BW

Sensibilisierung von Schülerinnen und Schülern sowie von Lehrkräften für Datenschutzfragen.

Ich selbst und unser Leitender Beamter Jan Wacke besuchten ebenfalls den Stand und führten zahlreiche spannende Gespräche. Unser Team nutzte auch die Gelegenheit, um sich über aktuelle Trends und Entwicklungen im Bildungsbereich zu informieren und mit den Praktiker_innen ins Gespräch zu kommen. So konnten sie viele Anregungen mitnehmen, die in zukünftige Projekte und Initiativen einfließen werden. Eine besondere Aufmerksamkeit gilt der Unterstützung von Schulen und der Schulverwaltung zur Beratung bei der Erstellung von Datenschutzdokumenten und der Durchführung von Schulungen und der Einsatz von Künstlicher Intelligenz (KI).

Die Didacta 2025 in Stuttgart war ein voller Erfolg und hat die Bedeutung des Datenschutzes im Bildungsbereich eindrucksvoll unterstrichen. Es wurde deutlich, dass wir auch weiterhin eine wichtige Rolle bei der Gestaltung datenschutzkonformer digitaler Lernumgebungen einnehmen müssen. Die gewonnenen Erkenntnisse und Kontakte werden dazu beitragen, unsere Arbeit noch effektiver und zielgerichteter zu gestalten.

Weitere Informationen

Der direkte Austausch mit Bürger_innen und mit einem spezialisierten Fachpublikum ist für uns wichtig. Neben der Präsenz auf der Didacta waren wir mit unseren Referent_innen auch wieder auf der re:publica, haben dort Vorträge gehalten – und aus Berlin auch neues Wissen mit in unsere Dienststelle gebracht. Auf dem 39. Chaos Communication Congress des Chaos Computer Clubs in Hamburg haben wir das mittlerweile legändäre DS-GVO-Quiz veranstaltet und wieder einmal festgestellt, dass die Commnunity bei vielen Themen schon eine Umdrehung weiter ist und tiefer nachgedacht hat, als wir es in unserer Bubble geschafft haben.

4.3. Level up your Privacy – Gamestate Festival Baden-Württemberg

Art. 57 Abs.1 Buchst. b), c) DS-GVO

In diesem Jahr haben wir erstmals am Gamestate Festival BW 2025 im Kulturwerk Stuttgart teilgenommen. Die Veranstaltung brachte professionelle Entwickler_innen, Studierende sowie Quereinsteiger_innen aus dem Land zusammen. Ziel war es, den lokalen Austausch zu fördern und Perspektiven sowie Entwicklungsmöglichkeiten für die Gaming-Branche aufzuzeigen.

Das Programm war auf intensive fachliche Diskussionen und interdisziplinären Austausch ausgelegt und umfasste ein vielfältiges Angebot aus Fachvorträgen, Roundtables, einer Podiumsdiskussion sowie einer abschließenden Networking-Party. Die vom Ministerium für Wissenschaft, Forschung und Kunst geförderte Veranstaltung wurde von der MFG Baden-Württemberg sowie weiteren Event-Partnern organisiert. Unsere Teilnahme zielte darauf ab, datenschutzrechtliche Anforderungen rund um das Gaming sichtbar zu machen und praxisnah zu vermitteln, denn gerade in dieser dynamisch wachsenden Branche, die von technischer Innovation und vielfältigen Datenverarbeitungsprozessen geprägt ist, spielt der Datenschutz eine zentrale Rolle.

Beim Gaming werden personenbezogene Daten in erheblichem Umfang verarbeitet. Nach Art. 4 Nummer 1 DS-GVO umfasst der Begriff „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen.“ Dementsprechend unterliegt jede Verarbeitung solcher Informationen den Anforderungen der DS-GVO, mit dem Zweck, die Rechte der betroffenen Personen zu schützen und eine Beeinträchtigung durch unzulässige oder intransparente Datenverarbeitungen zu verhindern. Bereits bei der Registrierung eines Spielerkontos werden üblicherweise verschiedene personenbezogene Daten verarbeitet. Dazu zählen etwa E-Mail-Adressen, Passwort, Nickname oder auch Altersangaben zur Altersverifikation. Hinzu kommen Daten, die beim Download von Spielern über Plattformen oder bei In-Game-Käufen anfallen.

Er erklärt gekonnt Datenschutz beim Gaming: LfDI-Referent Daniel Maslewski, LL.M., auf dem Gamestate Festival BW 2025. Bild: LfDI BW

Hierbei werden Kaufverhalten, Gerätedaten, Zahlungsinformationen und IP-Adressen verarbeitet. Auch die Speicherung von Spielständen erfolgt regelmäßig in einer Cloud, wodurch Speicher- sowie Accountdaten auf die Server des Anbieters übertragen werden. Weitere typische Verarbeitungsvorgänge betreffen beispielsweise Support-Anfragen, die häufig mit der Angabe von E-Mail-Adressen, Screenshots oder sogar Klarnamen verbunden sind, sowie Voice- und Text-Chats im Spiel, die eine Form der Live-Kommunikation darstellen.

Bei der Verarbeitung personenbezogener Daten müssen Verantwortliche die Grundsätze der Datenverarbeitung nach Art. 5 Abs.1 DS-GVO einhalten. Hierfür tragen sie auch die Dokumentations- sowie Nachweispflicht gemäß Art. 5 Abs. 2 DS-GVO. Gerade im Gaming-Kontext stellt die Umsetzung dieser Vorgaben jedoch eine Herausforderung dar. Zu berücksichtigen sind unter anderem komplexe Datenflüsse, zahlreiche Drittanbieterintegrationen oder Altersverifikationen. Zudem bestehen in dynamischen Spielekontexten häufig erhöhte Anforderungen an Transparenz- und Informationspflichten. Hinzu kommt der hohe Anspruch an Datensicherheit, um Nutzer_innen vor Cyberattacken zu schützen. Für Start-up-Unternehmen bedeutet das eine zusätzliche Belastung, da sie neben knappen Ressourcen und begrenztem Fachwissen auch komplexe rechtliche Vorgaben erfüllen müssen. Das erfordert in der Praxis, dass Verantwortliche sich zunächst ein Grundverständnis über die Datenverarbeitungsprozesse aneignen. Sie müssen vor allem verstehen, wer welche Daten zu welchem Zweck wie verarbeitet. Auf diesem Grundverständnis müssen Verantwortliche sich dann insbesondere fragen, welche Daten sie überhaupt verarbeiten dürfen und worüber sie betroffene Personen informieren müssen.

Es bedarf somit einer einschlägigen Rechtsgrundlage für die Verarbeitung personenbezogener Nutzerdaten, wofür in der Praxis häufig eine Einwilligung (Art. 6 Abs.1 Buchst. a) DS-GVO), eine Vertragserfüllung (Art. 6 Abs.1 Buchst. b) DS-GVO) oder die Verfolgung berechtigter Interessen (Art. 6 Abs.1 Buchst. f) DS-GVO) in Betracht kommen. Die Wahl der konkreten Rechtsgrundlage hängt dabei jedoch von den jeweiligen Umständen des Einzelfalls ab. Für die Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten nach Art. 4 Nr. 15 DS-GVO) ist zudem eine (zusätzliche) Rechtsgrundlage nach Art. 9 Abs. 2 DS-GVO erforderlich. Darüber hinaus verpflichtet die DS-GVO Verantwortliche nach Art. 13, 14 DS-GVO, betroffene Personen transparent über die Verarbeitung

Infokasten

Schulungen im Bildungszentrum BIDIB: https://www.baden-wuerttemberg.datenschutz.de/bidib-veranstaltungen/

ihrer personenbezogenen Daten zu informieren. Diese Informationspflichten dienen der Nachvollziehbarkeit und Prüfbarkeit. Spieler müssen daher klar und verständlich erfahren, wer ihre Daten verarbeitet, welche Daten betroffen sind und zu welchem Zweck die Verarbeitung erfolgt. Erfolgt die Datenerhebung unmittelbar beim Spieler, so gilt Art. 13 DS-GVO. Werden Daten hingegen nicht direkt beim Spieler erhoben (z. B. Dritterhebung), so müssen die Anforderungen von Art. 14 DS-GVO beachtet werden. Eine Information hat im letztgenannten Fall grundsätzlich innerhalb eines Monats zu erfolgen. Die Erfüllung der Informationspflichten kann dabei auch über einen klaren Verweis auf die ausführliche Datenschutzerklärung auf der Homepage erfolgen (sog. Medienbruch).

Zur Erfüllung der datenschutzrechtlichen Anforderungen sollte Datenschutz von Beginn an mitgedacht und bereits fest in die Spieleentwicklung integriert werden. Bereits in der Konzeptphase ist zu planen, welche Daten tatsächlich benötigt werden und wie diese bestmöglich durch technische und organisatorische Maßnahmen geschützt werden können. Zur notwendigen Information der Spieler sollte eine einfache Sprache verwendet und Datenschutzhinweise sollten gut sichtbar – etwa beim ersten Start des Spiels und damit vor der Datenerhebung – platziert werden. Dabei sollte insbesondere berücksichtigt werden, dass Kinder im Datenschutzrecht als besonders schützenswert sind und für sie mitunter besondere Bestimmungen gelten (vgl. Art. 8 DS-GVO). Entsprechend sollten Hinweise altersgerecht formuliert, Elternfreigaben eingeholt und ggf. Altersüberprüfungen vorgesehen werden. Wichtig ist, Datenschutz nicht als reine Pflicht, sondern vielmehr als Mehrwert zu verstehen. So kann die Einhaltung datenschutzrechtlicher Vorgaben das Vertrauen der Nutzer stärken, die Cybersicherheit erhöhen und letztlich zu einem Qualitätsmerkmal im Wettbewerb werden. Wir unterstützen Verantwortliche beratend bei der Einhaltung datenschutzrechtlicher Anforderungen und helfen ihnen beim Aufbau datenschutzrechtlicher Kompetenzen mit kostenfreien Schulungen in unserem hauseigenen Bildungszentrum für Datenschutz und Informationsfreiheit Baden-Württemberg – BIDIB.

4.4. Veranstaltungen zum Datenschutz als Kulturaufgabe

Art. 57 Abs. 1 Buchst. b), d), i) DS-GVO

Uns mit engagierten Akteuren im Feld der Digitalpolitik und Medienbildung zu vernetzen, um für unser Thema Datenschutz als modernes Grundrecht zu sensibilisieren, ist für uns im Bereich Datenschutz als Kulturaufgabe weiterhin maßgeblich. Weil die digitale Infrastruktur unserer aller Lebensvollzüge, sei das im Privaten, sei das im öffentlichen oder staatlichen Handeln oftmals in der Hand von sehr wenigen privaten Unternehmen liegt, geraten auch die Bedingungen für eine handlungsbefähigende, starke Demokratie mehr und mehr in den Blick. Durch KI beschleunigt sich diese Machtbündelung und der Druck auf die Einzelnen, auf staatliche und private Institutionen sowie auf das freie Marktgeschehen. Durch Kooperationen können wir in unserer Sensibilisierungs- und Aufklärungsarbeit, in welcher wir auch die Geschäftspraktiken von Technologieanbietern nach Art. 57 DS-GVO Abs. 1 Buchst. i) in den Blick nehmen, Kräfte bündeln, neue Zielgruppen ansprechen und uns aktiv in Diskurse einbringen. Wir vernetzen uns in die Stadtgesellschaft, Wissenschaft und Kunst hinein und interessieren uns an dieser Stelle auch ganz allgemein für die gesellschaftlichen Auswirkungen von Künstlicher Intelligenz und Digitalisierung. Denn personenbezogene Daten und ihre Auswertung nehmen in der Digitalisierung eine zentrale Rolle eine.

4.4.1. Das 14. Forum Digitale Lebenswelt in Speyer

Wir waren am 28. und 29. April wieder als Kooperationspartner in Speyer. In der 14. Ausgabe des Forums Digitale Lebenswelt gingen Expertinnen und Experten der Frage nach, wie kluger Datenschutz, effektive Datensicherheit und zielgenaue Datennutzung in zentralen staatlichen Aufgabengebieten verknüpft werden können. Aus Baden-Württemberg bespielten wir das Panel KI und Informationsfreiheit mit zwei Vorträgen zur Anwendung von KI in der „Automatischen Texterkennung von Handschriften im Projekt OCR-BW“ von

Dorothee Huff, Universitätsbibliothek Tübingen, und zur „KI-gestützte Informationsgewinnung aus Archivgut beim Aufbau des bundesweiten Digitalportals Wiedergutmachung nationalsozialistischen Unrechts“ von Nastasja Pilz, Landesarchiv Baden-Württemberg. Das nächste Speyerer Forum findet am 16. und 17. April 2026 wieder an der Deutschen Verwaltungsuniversität Speyer und online statt.

4.4.2. GameChanger Datenschutz

Erstmalig haben wir mit dem Internationalen Trickfilm-Festival Stuttgart (ITFS) kooperiert und zusammen ein Expert_innen-Panel für das Begleitprogramm zum Wettbewerb aufgesetzt. Wir sprachen damit gezielt ein junges Publikum und deren Eltern an. Unsere Fragen waren: Wie kommen wir mit der Games-Communitiy ins Gespräch? Wie geht Online-Gaming sicher und selbstbestimmt? Welche Daten werden wann von wem erfasst, wohin fließen diese, wer nutzt sie und für was? Ein jugendlicher Gamer nahm uns in einer Videosequenz mit in seinen Chat und zeigte, wo mit Scamming zu rechnen ist. In kurzen Vorträgen warfen dann Alvar Freude und Tamara Damjanović, Fachleute für technisch-organisatorischen Datenschutz und fürs Gaming aus unserer Dienststelle, sowie Kilian Brand, FSJler bei YoungData unter dem Dach des LfDI Rheinland-Pfalz, Schlaglichter auf den Schutz vor solchen übergriffigen oder betrügerischen Aktivitäten in Online-Communities (zu Gaming s. auch Kap. 4.3.). Anschließend haben wir mit dem Publikum diskutiert: Wie ist ein verantwortungsvoller Umgang mit persönlichen Informationen beim Gaming möglich? Wie schütze ich mich und Informationen über andere?

Wir danken den ITFS-Macherinnen für diese tolle Zusammenarbeit. Ein weiterer Kooperationspartner war das Jugendportal YoungData.de, eine Initiative der Datenschutzkonferenz der Länder, an der wir uns auch redaktionell beteiligen.

4.4.3. Vernetzung mit lokalen Bildungspartnern

Interessierte konnten sich im Mai zu einem Blick hinter die Kulissen über die der VHS Stuttgart anmelden. Sie erhielten Einblick in unsere tägliche Arbeit durch mich als Dienststellenleiter sowie durch weitere Kolleg_innen. Wir haben es ganz praktisch gehalten und darüber gesprochen, was aktuell auf dem Schreibtisch eines LfDI liegt, was eigentlich technisch-organisatorischer Datenschutz ist und inwieweit die Informationsfreiheit die Möglichkeiten unterstützt, sich als Individuum oder Interessensgruppe in das Gemeinwesen einzubringen. Wir haben auch einen Blick auf Europa

Datenschutz als modernes Grundrecht: Transparenz und Prüfbarkeit von Künstlicher Intelligenz zum Wohle aller, Chancengleichheit, Fairness, Diskriminierungsminimierung, Meinungsvielfalt, Medienvielfalt, Freihalten öffentlicher (digitaler) Räume, Recht auf freie Meinungsäußerung, Recht auf (digitale) Bildung, Wettbewerbserhalt und marktwirtschaftliche Prinzipien für den digitalen Raum, Interessensausgleich und Ausgleich von Macht in der digitalen Gesellschaft

Illustration: Y. Dwiputri
Bilder: LfDI BW

Internationales Trickfilm-Festival Stuttgart: Tamara Damjanović (2.v.l.), Kilian Brand vom LfDI Rheinland-Pfalz (3.v.l.) und Alvar Freude (rechts) im Gespräch mit Moderator Constantin Schnell über Gaming.

LfDI-Abteilungsleiter Alvar Freude bei seinem Vortrag über Cookies – und wie man bei Website-Anbietern einfach Auskunft verlangen kann über die personenbezogenen Daten, die sie verarbeiten.

LfDI-Infostand beim „Fest der digitalen Freiheit“ in der Stadtbibliothek Stuttgart. Auf die Wand projiziert: Die Lichtinstallation „Data to Light“ von Florian Mehnert.

geworfen und berichtet, was etwa unsere Mitarbeit in Unterarbeitsgruppen des Europäischen Datenschutzausschusses (EDSA) für Auswirkungen auf den gelebten Datenschutz bei uns im Land hat. Spannende Abstimmungsprozesse zwischen Landes- und europäischer Ebene wurden greifbar. Nach jedem Vortrag gab es Gelegenheit zum Austausch – und wir als lernende Behörde nahmen Fragen auf und Anregungen mit.

Mit der Hochschule der Medien Stuttgart (HdM) verbindet uns an der Schnittstelle von Datenschutzrecht und digitaler Ethik bereits eine langjährige produktive Zusammenarbeit. Bei der diesjährigen IDEepolis waren wir Kooperationspartner und haben uns mit meinem Vortrag „Assistierte Bildung? Vorgaben des Datenschutz- und KI-Rechts für den Bildungssektor“ ins Tagungsthema „KI und Bildung: Künstliche Systeme in Unterricht und Lehre“ eingebracht. Wie schon beim Vernetzungstreffen „KI und Demokratie“, organisiert von der Landeszentrale für politische Bildung Baden-Württemberg (LpB) im Haus der Wirtschaft waren wir auch auf dem Campus der HdM mit einem eigenen Stand vor Ort. Beim Vernetzungstreffen der LpB stellte ich „Leitlinien zum Umgang mit KI in (öffentlichen) Institutionen“ vor und sprach mit dem stellvertretenden Direktor der LpB Reinhold Weber. Auf beiden Veranstaltungen haben wir nicht nur unsere Perspektive eingebracht, sondern auch wichtige Impulse für unsere Arbeit und zu Kulturtechniken des Digitalen erhalten.

4.4.4. Fest der digitalen Freiheit

In der Stadtbibliothek Stuttgart sind wir regelmäßig mit Vorträgen zu Gast, so sprach ich dort im Mai auf Einladung des CCC Stuttgart zum Thema „Datenschutz, Informationsfreiheit, KI: Aktuelle Themen des LfDI".

Ein Highlight in der Zusammenarbeit war im Oktober dann das „Fest der digitalen Freiheit. Aktionstag pro Datenschutz und contra Fake News“. Als Kooperationspartner stellten wir mit weiteren Institutionen ein informatives, künstlerisches, medienpädagogisches und aktivierendes Programm für alle Altersgruppen auf die Beine. So wurde etwa für die ganz jungen Menschen aus Kinderbüchern vorgelesen und dabei Themen der digitalen Ethik angesprochen, der Verein „digitalcourage“ hat mit „Muurmel – Die Erklärbahn zum Thema Datenschutz und Digitale Mündigkeit“ das Thema Filterblasen erklärt, und die Landesmedienanstalt und die Verbraucherzentrale haben ihre Angebote für die Verbraucher_innen vorgestellt.

Im Max-Bense-Forum gaben unsere Fachleute Alvar Freude und Karoline Nutz in Vortrag (s. auch Kap. 2.5.) und Fragerunde sehr nützliche Hinweise, wie man herausfindet, welche Tracker beim Surfen im Netz auf dem eigenen Browser landen und welche Werkzeuge das Datenschutzrecht an die Hand gibt, um sich dagegen zu wehren und bei den Betreiberfirmen auf die Löschung der eigenen Daten zu dringen. Im Showroom konnte unterdessen „Colliding Objects“ aus unserer Kooperation mit der Macromedia Hochschule gespielt werden (vgl. LfDI BW, 40. Tätigkeitsbericht Datenschutz 2024) – ein Spiel, das unter anderem zeigt, wie Verhaltensdaten der Spielenden auslesbar werden, welche es erlauben, Nutzende z. B. in Werbezielkategorien zu sortieren. Wie stark hier Datenhändler aktiv werden, haben die preisgekrönten Journalist_innen von netzpolitik.org und dem Bayerischen Rundfunk in der Vergangenheit deutlich gezeigt (s. https://netzpolitik.org/databroker-files/). Der Film der Ludwigsburger Filmstudentin Michaela Kobsa-Mark „all eyes on you“ zur Videoüberwachung im Stadtraum stellte die Frage, ob algorithmenbasierte Kameraüberwachung durch ein gebiastes Training der Modelle eine Diskriminierung bestimmter Passantengruppen ungewollt weiterhin „abbildet“ oder möglicherweise noch verstärkt. Wir führten mit ihr ein Publikumsgespräch, in welchem Zuschauende auch den Bogen zur Verfahrensübergreifenden Recherche- und Analyseplattform VeRA spannten. Und am Abend konnte man der Leseperformance quer durch die Überwachungsliteratur lauschen: „Art of Being…Observed“ (vgl. LfDI BW, 39. Tätigkeitsbericht Datenschutz 2023).

Der Aktionstag ermöglichte es dem Publikum, Informationen aus verschiedensten Kontexten miteinander in Bezug zu setzen. Der analoge Austausch wurde generationsübergreifend möglich, gemeinsam machten wir den Versuch über die jeweiligen Slots hinweg ein vielstimmiges Gesamtbild zum Thema digitale Grundrechte zu entwerfen.

Infokasten

Dokumentiert ist die Veranstaltung hier: https://www.baden-wuerttemberg.datenschutz.de/fest-digitale-freiheit-18-oktober/

Veranstaltungsplakat KI-Woche 2025.
Gestaltung: Y. Dwiputri

4.4.5. wer/m nutzt KI? – KI-Woche 2025

Art. 57 Abs.1 Buchst. b), d), i) DS-GVO

Am 3. und 4. November fand unsere diesjährige KI-Woche statt. Die Teilnahme war wieder vor Ort – noch im Foyer unserer „alten" Dienststelle in der Lichtkunst von Florian Mehnert – und online möglich, und wie in den vorherigen Ausgaben kostenfrei. Der Zuspruch des Publikums war so groß, dass wir für den ersten Tag die Anmeldung aussetzen mussten: Auf sehr großes Interesse stieß unser Keynote-Speaker Rainer Mühlhoff mit seinem Vortrag „KI, Macht, Daten", in welchem er sehr grundsätzlich auf den Zusammenhang von Big Data, prädiktiver Analytik und der daraus resultierende Zukunftsmacht der großen Tech-Unternehmen zu sprechen kam. Ist KI ein Werkzeug – oder viel eher ein soziotechnisches System? Wenn ich Daten von mir preisgebe, betrifft das tatsächlich nur mich selbst – oder unterstütze ich damit auch die Vorhersagemacht über alle anderen? Was machen die Stakeholder mit dieser Vorhersagemacht? Mache ich mit meiner eigenen Datenpreisgaben Minderheiten erst sichtbar? Was ist, wenn sich Big Tech, also Privatwirtschaft, und Staat so sehr annähern, dass eine effektive Regulierung des einen durch den anderen nicht mehr gut möglich scheint? Zu diesen und vielen weiteren Fragen führten wir ein spannendes Gespräch, das man, wie auch die anderen Vorträge der KI-Woche, auf unserer Website ansehen kann.

Infokasten

Vorträge vom ersten Tag der KI Woche 2025: https://tube.bawü.social/w/xbmuQ9ePRYFE-7Ni1URwcKG; Vorträge vom zweiten Tag der KI-Woche 2025: https://tube.bawü.social/w/xbmuQ9ePRYFE7Ni1URwcKG

CR-online.de Blog: AI hot mess – Meta at German courts and the troubling state of EU regulation – CR-online.de Blog: https://www.cr-online.de/blog/2025/09/07/ai-hot-mess-meta-at-german-courts-and-the-troubling-state-of-eu-regulation/

Wer hat welche Interessen an KI?

Regulierung hat in Teilen der Öffentlichkeit und Politik derzeit keinen guten Klang. Doch dass sie Voraussetzung für Freiheitsrechte ist, dies sollten die Datenschutzaufsichten selbstbewusster für sich in Anspruch nehmen, so schrieb es uns Rainer Mühlhoff, der gemeinsam mit Hannah Ruschemeier auch zu den Grundlagen für ein modernes Datenschutzrecht forscht, regelrecht ins Stammbuch. Datenschutz kann die Voraussetzung für einen gesellschaftlichen Interessens- und Machtausgleich sein, kann die Rechte von Minderheiten schützen, freie Meinungsbildung und Meinungsäußerung ermöglichen, den öffentlichen Raum und einen regelbasierten digitalen Markt stärken. Regeln schützen (auch unternehmerische) Grundrechte und ermöglichen erst einen modernen demokratischen Staat.

Rainer Mühlhoff hat die von ihm aufgeworfenen Fragen zum Anlass genommen, schließlich alle Datenschützer_innen direkt anzusprechen: Datenschutzrecht als Individualrecht müsse erweitert werden um den Schutz vor systemischen Risiken, die die Gesellschaft als Ganzes betreffen. Eine Frage lautete hier: Gibt es eine Regulierungslücke zwischen einem für einen bestimmten Zweck trainiertem KI-Modell und dessen Weitergabe zu einer anderer Verwendung?

Vor der Keynote bestand die Möglichkeit in Workshops hands-on zu KI und Datenschutz ins Gespräch zu kommen: Vorgestellt wurde von unseren Referent_innen der lokale Einsatz von Sprachmodellen, Voraussetzungen für den Einsatz von KI im Bildungsbereich, Rechtsgrundlagen für den Einsatz von KI in Unternehmen und die datenschutzrechtlichen Vorteile des Einsatzes von RAG-Systemen (s.oben Kap. 2.4.).

Im Blick: Geschäftspraktiken von Palantir

Am ersten Abend hatten wir auch den Filmemacher Klaus Stern vor Ort, der seinen vielbeachteten Dokumentarfilm „Watching You – Die Welt von Palantir und Alex Karp" zeigte. Dass die Änderung des Polizeigesetzes in Baden-Württemberg für einen möglichen Einsatz der bei Palantir gekauften Datenanalysesoftware als Grundlage für VeRA (Verfahrensübergreifendes Recherche- und Analyseplattform) beinahe zeitgleich im Landtag zu besprechen war, haben wir bei der Programmplanung noch nicht gewusst. Der Film erlaubte jedenfalls einen differenzierten Blick auf Firmengründer und Firma: auf die Geschäftspraktiken und das unter-

Infokasten

Neue Anforderungen an politische Werbung durch die TTPW-Verordnung – kompakte Hilfestellung für politische Akteure: https://www.baden-wuerttemberg.datenschutz.de/hilfestellung-ttpw-verordnung/

FAQ: Verordnung über die Transparenz und das Targeting politischer Werbung: https://www.datenschutz-berlin.de/themen/werbung/politische-werbung/
Aus den FAQ Berlin: „Was ist Targeting? In den Internetwerbenetzwerken und durch die großen Onlineplattformen werden u. a. mittels Trackingtechnologien personenbezogene Daten erhoben, ausgewertet und bestimmten Interessenkategorien zugeordnet. Dadurch entstehen umfangreiche Interessens- und Verhaltensprofile, die es den Werbenden ermöglichen, auf Websites, Onlineplattformen oder über Social-Media-Kanäle mithilfe von Targetingverfahren maßgeschneiderte Inhalte an ausgewählte Adressat_innen auszuspielen. Diese sollen dadurch so effektiv wie möglich mit der Werbung erreicht werden, d. h. die Instrumente sind dahingehend optimiert, die Adressat_innen so zu beeinflussen, wie von den Werbenden gewünscht."

nehmerische Bestreben, sich im globalen Markt als alternativlos für die jeweiligen staatlichen Sicherheitsarchitekturen darzustellen und damit (Daten-)Macht sehr stark auf das eigene Unternehmen zu vereinen.

Dabei drängten sich hochaktuelle datenpolitische Fragen auf: Läuft die Software geschlossen lokal und was bedeutet es, wenn Palantir-Mitarbeitende im Regelbetrieb vor Ort sein müssen, um das System zu pflegen und aktuell zu halten, wie es im Film das Beispiel Hessen zeigt? Inwiefern scheint realistisch, die Software unter dem Stichwort der digitalen Souveränität bloß als Übergangslösung zu implementieren, wenn die übrigen Softwarearchitekturen erst aufwendig darauf zugeschnitten werden müssen? Die Themen, die der Film auffächert, haben wir in der anschließenden Diskussion bezogen auf unsere datenschutzrechtliche Perspektive hier in Baden-Württemberg intensiv diskutiert.

Was darf benutzt werden?

Am nächsten Tag sprach Juniorprofessorin Paulina Jo Pesch zu einem Urteil des Kölner Oberlandesgerichtes vom Sommer 2025, das die Datenschutzszene sehr beschäftigt hat. Die Verbraucherzentrale NRW hatte eine einstweilige Verfügung zum angekündigten KI-Training mit (zurückliegenden) öffentlichen Social-Media-Posts durch Meta angestrengt – und war damit im Eilverfahren gescheitert. Das Hauptsacheverfahren ist noch offen. Paulina Pesch stritt dafür, dass das Training von KI-Modellen mit personenbezogenen Daten nicht zu leichtfertig als DS-GVO-konform einzustufen sei und bezog sich auch auf den risikobasierten Ansatz der KI-Verordnung (KI-VO): besondere Kategorien personenbezogener Daten und Daten von Minderjährigen seien zum Beispiel nicht ausreichend in der Risikobewertung durch das OLG Köln berücksichtigt. Dagegen hob sie das Forschungsprivileg hervor, unter welchem man es Meta gerichtlich hätte erlauben können, KI mit Nutzendendaten zu trainieren, um mögliche Risiken besser bewerten zu können. Ähnlich wie auch Mühlhoff sah sie das Training einer Mehrzweck-KI für eine allgemeine Verwendung jedoch kritisch und forderte mehr Kompetenzaufbau zu auch möglichen systemischen Risiken von KI bei allen Entscheidungsträger_innen, bevor solche breit trainierte Mehrzweck-KI-Modelle auf die Straße kämen.

Wem nutzt KI – wer nutzt KI zu was?

Im Wahljahr 2026 muss von besonderem Interesse sein, politisches Targeting auf die Rechtmäßigkeit seiner Anwendung hin zu überprüfen. Muss man damit rechnen, dass Wählergruppen gezielt und mit Falschdarstellungen auf Social Media angesprochen werden? Wer kommt wie an die Nutzendendaten und auf welcher Rechtsgrundlage? Inwieweit ermöglichen KI-generierte Inhalte eine propagandistische Ansprache? Was sehen junge Wähler_innen z. B. auf TiKToK und in welcher Frequenz? Ist „Richtigkeit" von Bildinhalten überhaupt eine Kategorie?

Der europäische Gesetzgeber hat seit den us-amerikanischen Erfahrungen um den Datendienstleister Cambridge Analytica und seit den Versuchen zur gezielten Beeinflussung der Brexit-Abstimmung die technischen Möglichkeiten, Gruppen zu klassifizieren und mit spezifischen zugeschnittenen und auch einander widersprechenden Werbebotschaften zu bespielen, im Blick. Auf den Digital Services Act (DSA), der es den Betreibern von politischem Targeting erstmals vorschreibt, ihre

Vorschlagsalgorithmen für die Forschung offenzulegen, folgte als spezifischere regulatorische Antwort im letzten Jahr die Verordnung über die Transparenz und das Targeting politischer Werbung (TTTW-VO), die seit Oktober 2025 in Deutschland gilt.

Die gemeinsame Verantwortung für die Verarbeitung von personenbezogenen Daten macht nötig, dass sich Parteien als sogenannte Sponsoren, wenn sie Wahlwerbung gezielt auf Social Media ausspielen möchten, mit der neuen Verordnung beschäftigen.

Hierzu hat die Berliner Datenschutzbeauftragte Meike Kamp FAQs bereitgestellt (s. Infokasten). Sie kam nicht nur als Landesbeauftragte, sondern auch als Vorsitzende der Datenschutzkonferenz 2025 zu uns, um einen Überblick zu dieser neuen Verordnung und zur Systematik der verschiedenen Rechtsakte, die politisches Targeting adressieren, zu geben. Auch adressierte sie die systemischen Risiken durch Targeting und Anzeigenschaltungsverfahren in der sozialen Kommunikation im Netz und sprach über die Schwierigkeiten der Rechtsdurchsetzung und zu Strittigkeiten bezüglich möglicher Regulierungslücken (wenn etwa Content durch Influencer„organisch“ und unbezahlt algorithmenbasiert ausgespielt wird).

Doch zuvor beschrieb Rechtsanwältin Jessica Flint sowohl aus ihrer Forschung (– so im Rahmen ihrer Dissertation zu Fake News im Wahlkampf am Beispiel von Facebook aus rechtlicher Perspektive –) als auch aus ihrer anwaltlichen Praxis, wie sich die großen Plattformen in Bezug auf politisches Targeting einer Regulierung weitgehend zu entziehen suchen. Unter dem Titel „Wer manipuliert meine politische Meinung?“ holte sie uns prononciert die machtvolle Ausspielung extremer und extremistischer politischer Inhalte über Social Media ins Bewusstsein.

Die Bestandsaufnahmen der gehörten Beiträge von Mühlhoff, Stern, Pesch, Flint und Kamp machte offenbar, wie akut der Handlungsbedarf ist, um für gute Regeln für den digitalen Raum, in welchen sich öffentliches Handeln und politische Kommunikation mehr und mehr verlegen, selbstbewusst zu streiten bzw. die Regulierung, welche die EU bereits förderlich auf den Weg gebracht hat, im Namen von Gemeinwohl, Interessensausgleich und Chancengleichheit sowie der individuellen Freiheitsrechte zur Wirkung zu bringen.

Mit dem letzten Panel zur Digitalen Souveränität stellten wir uns die Frage, was dies in der Praxis bedeutet, wie man KI also besser und unabhängiger von den großen Playern machen kann und was es dafür an regulatorischen Voraussetzungen braucht.

Wie geht es anders? Digital souverän?!

Der Publizist und Medienwissenschaftler Martin Andree betitelte seinen Vortrag zugespitzt: „Game over Democracy? Willkommen in der Digitalokratie“. Er führte die KI-Woche mit der Keynote zum Panel Digitale Souveränität thematisch eng und warb mit Vehemenz für realistische Auswege aus der Abhängigkeit von BigTech. Er zeichnete nach, wie die großen Plattformen zu ihren Privilegien kamen, welche es ihnen überhaupt erst erlaubt hatten, Monopole aufzubauen, und legte dar, wie sie (wieder) einzuhegen sein könnten in die europäischen Rechtsstrukturen. So sprach er über die

Bild: LfDI BW

LfDI Tobias Keber über den KI-Fernsprecher:

Der KI-Fernsprecher, den uns die Landesmedienanstalt temporär ausgeliehen hat, illustriert auf herausragende Weise, wie es gelingen kann, mit Mitteln der medienpädagogisch-künstlerischen Intervention neue Techniken zu nutzen und sich dabei zu ihnen ins Verhältnis zu setzen, diese auch zu hinterfragen. Während unserer KI-Woche 2025 konnten die Teilnehmenden den intelligenten Fernsprecher ausprobieren und mit fiktiven Menschen aus der Vergangenheit „sprechen“, ihre Geschichten „hören“, sich Fragen stellen lassen und selbst Fragen zum Zeitgeschehen stellen. Möglichkeiten und Grenzen der künstlich generierten „Gegenüber“ wurden in dieser Interaktion erlebbar. Und der Datenschutz war bei der Frage um das Training von KI mit Spracheingabedaten klar adressiert.

Rainer Mühlhoff im Gespräch mit LfDI Tobias Keber nach seinem Eröffnungs-Vortrag der KI-Woche 2025 „KI, Macht, Daten“.

Paulina Jo Pesch im Gespräch über KI-Modelle und Trainigsdaten.

LfDI Tobias Keber und Filmemacher Klaus Stern im Gespräch über seinen Film „Watching You – Die Welt von Palantir und Alex Karp“. Alle Bilder: LfDI BW

Inwieweit ermöglichen KI-generierte Inhalte eine propagandistische Ansprache?

Ist „Richtigkeit“ von Bildinhalten überhaupt eine Kategorie?

Was sehen junge Wähler_innen z. B. auf TiKToK und in welcher Frequenz?

Wer kommt wie an die Nutzerdenaten und auf welcher Rechtsgrundlage?

Illustration: Y. Dwiputri

Unterschiede bei der Regulierung von Medien und Intermediären, den möglichen Nutzen von offenen Standards und auch davon, ob nicht die Haftung der Plattformen für Inhalte, mit denen sie Geld verdienen, ein Hebel sein könnte, sie stärker als bisher in die Verantwortung zu nehmen. Flankiert war dieser Vortrag vom Impuls des Präsidenten der Landesmedienanstalt Wolfgang Kreißig: „Der schwere Weg zurück – Wertebasierte Medienregulierung vs. Macht der Plattformen“. In der Analyse dem zuvor Gehörten sehr verwandt skizzierte auch er mögliche konstruktive Lösungsansätze aus der diagnostizierten Gefahr für Demokratie und Medienvielfalt und stellte entsprechend Ansatzpunkte des Medienstaatsvertrages vor.

Es braucht vermutlich beides, um einer „Digitalokratie“ die Absage zu erteilen: Die Regulierung des digitalen Marktes, damit die Macht, Zugangsregeln für den öffentlichen Diskurs zu definieren, nicht allein dem privaten Sektor überlassen bleibt, sowie eine vielfältige und demokratischen Spielregeln verpflichtete Entwicklung digitaler Räume und Infrastrukturen mit breit ausgehandelten Zielsetzungen; eine gute Praxis der Innovation durch regulatorische Leitplanken.

Für uns Datenschützende ist hier ein guter Punkt einzuhaken. Können wir durch einen frühen Einbezug zu einer datenschutzkonformen, KI-Verordnung-konformen und datensicheren KI-Entwicklung und Anwendung etwas zu einer souveränen technischen Infrastruktur beitragen? Und das „made in BW“?

Unser KI-Beauftragter Peter Nägele vertrat auf dem abschließenden Podiumsgespräch, das ich moderierte, unser geplantes interdisziplinär ausgerichtetes Projekt Mind.bw., das in Baden-Württemberg KI-Reallabore stärken will. Mind.bw steht für „Menschenzentrierte Innovation – Netzwerk Digitalisierung Baden-Württemberg“. Wir diskutierten über staatliche Rahmenbedingungen und das „richtige“ Maß an Regulierung, das notwendig ist, um nicht nur KI-Anwendungen, sondern vertrauenswürdige KI-Anwendungen zu machen, die Menschen tatsächlich nutzen wollen.

Mit diesen Ausblicken auf Handlungsoptionen verabschiedeten wir uns aus der diesjährigen KI-Woche und freuen uns auf den 2. und 3. November 2026. Dann findet unsere KI-Woche 2026 statt.

4.5. Online-Angebot und digitale Kommunikation

Art. 57 Abs.1 Buchst. b), d), i) DS-GVO

Auch in diesem Jahr haben wir durch unsere Presse- und Öffentlichkeitsarbeit über unsere Arbeit informiert, für Themen sensibilisiert, aufgeklärt und Informationen bereitgestellt sowie am Diskurs über Datenschutz teilgenommen.

4.5.1. Podcast „Datenfreiheit“

Unser Podcast Datenfreiheit hat sich als Format etabliert und wird gehört. Unsere Extrafolgen erfreuen sich ebenfalls größerer Beliebtheit. So haben wir ein Format entwickelt, bei dem wir zusammen mit dem Datenschützer und Lehrbeauftragten Rudi Kramer über aktuelle datenschutzrechtliche Themen sprechen und die Vielzahl von Rechtsprechungen und Publikationen einordnen. Zudem laden wir Gäste ein, um mit ihnen ein Thema ausführlicher zu besprechen. Zwei besondere Folgen sollen hier hervorgehoben sein. Mit der renommierten Bildungsforscherin Ulrike Cress aus Tübingen sprachen wir über KI in der Schule und wie es gelingen kann, pädagogisch nachhaltige KI-Tools für den Bildungsbereich zu entwickeln. Unbedingt nachzuhören ist auch unser Gespräch mit der Psychologin und Digitalisierungsexpertin Marina Weisband über die Relevanz öffentlicher, demokratischer Räume für die Teilhabe und die Bildung junger und erwachsener Menschen, über ihr Projekt „aula“ für Schulen und über Social Media und Altersgrenzen. Marina Weisband kam zur 50. Podcastfolge, wir sind sehr dankbar für dieses großartige Gespräch. Auch empfehlen wir sehr die Podcastfolge, in der wir zusammen mit der Vorständin der Verbraucherzentrale Baden-Württemberg Cornelia Tausch über gemeinsame Schnittstellen in unseren Arbeitsfeldern und mögliche gemeinsame Projekte sprechen.

Infokasten

Alle Podcasts zum Nachhören: https://www.baden-wuerttemberg.datenschutz.de/datenfreiheit/

Bei der Aufzeichnung des LfDI-Podcast „Datenfreiheit“, Folge: 48: „KI in der Schule“: LfDI Tobias Keber und Bildungsforscherin Ulrike Cress. Bild: LfDI BW

4.6.2. Microblogging: Mastodon

Wir schätzen die direkte Kommunikation und unterstützen dies mit einem eigenen Mastodon-Server. Auf diesem können öffentliche Stellen in Baden-Württemberg und Stellen mit Bezug zu öffentlichen Aufgaben einen Account einrichten. Über 150 Accounts sind auf dem Server eingerichtet, rund 100 Accounts sind regelmäßig aktiv. Wir nutzen unsere Accounts, um auf aktuelle Datenschutzthemen einzugehen und über unsere Themen und Veranstaltungen zu informieren. Wir berichten von unserer Arbeit und suchen den Austausch. Der LfDI-Accounts hat rund 7300 Follower, der LfDI-Pressestellenaccount knapp über 1500 Follower.

Dieser Microbloggingdienst ist Teil des Fediverses. Weiterhin ist nicht klar, ob Mastodon etwa eine tatsächliche Alternative für die gewinnorientierten Plattformen der großen Technikkonzerne sein kann. Wir stellen fest, dass Diskussionen intensiver stattfinden, sich auch sukzessive neue Accounts auf unserem Server anmelden. Auch nehmen wir wahr, dass im Zuge der gesellschaftlichen Diskussionen über digitale Souveränität nicht-kommerzielle Plattformen stärker in den Fokus rücken. Für uns ist Mastodon bislang sehr positiv zu bewerten. Wir freuen uns darüber, dass immer mehr Menschen und öffentliche Stellen alternative Kommunikationsorte für sich entdecken und diese nutzen. Weiterhin bieten wir baden-württembergischen Stellen an, bei uns einen Mastodon-Account einzurichten.

4.6.3. Videoplattform PeerTube

PeerTube ist wie YouTube eine Plattform, auf der Videos zur Verfügung gestellt werden können, und Teil des Fediverse. Die Videoplattform haben wir derzeit noch nicht für alle interessierten öffentlichen Stellen öffnen können, haben dazu aber kleine Pilotprojekte umgesetzt, etwa mit der Landeszentrale für politische Bildung (LpB) und im Zuge einer Kooperation mit den Datenschutzkolleg_innen aus Rheinland-Pfalz. Wir stellen fest, dass es einen Bedarf bei öffentlichen Stellen gibt, datenschutzfreundlich Videos zur Verfügung zu stellen, uns erreichen regelmäßig Anfragen dazu. Wir werden im kommenden Jahr versuchen, mit der Öffnung von PeerTube voranzukommen.

Wir streamen auf PeerTube live Veranstaltungen und stellen Aufzeichnungen zur Verfügung. Wir sind sehr zufrieden damit, dass wir Bewegtbild-Content datenschutzfreundlich anbieten können. Die Resonanz ist sehr erfreulich. PeerTube wird kontinuierlich weiterentwickelt, sodass wir davon ausgehen können, dass die Nutzbarkeit und die Nutzung künftig weiter steigt.

4.6.4. Internetangebot

Im vergangenen Jahr haben wir ein Refresh der Seite vorgenommen und arbeiten an weiteren Verbesserungen für die Nutzenden. Die Öffentlichkeitsarbeit unterstützt die Fachlichkeit des Hauses und will möglichst viele Menschen ansprechen. Wir gehen davon aus, dass durch diese Art der Wissenslieferung manche Beratungsanfrage uns erst gar nicht erreicht. Wir liefern auf unserer Website aktuelle Beiträge, Handreichungen, FAQ und Checklisten. Wir hoffen, dass verantwortliche Stellen durch die Würdigung der Inhalte ihre Anwendungen und Angebote datenschutzfreundlicher anbieten und wir wirksam dabei helfen können, Datenschutzverstöße zu vermeiden.

Die Nachfrage an Wissen ist vorhanden, unsere Angebote werden genutzt. Weiterhin gehört unser Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ mit über 30.000 Aufrufen im vergangenen Jahr zu den beliebtesten Seiten. Unser Angebot zur „digitalen Kehrwoche“ wurde ebenfalls häufig aufgesucht, der „Art. 17 DS-GVO Selfcheck“ etwa hatte rund 8000 Aufrufe.

Unser Bildungszentrum BIDIB wurde rund 8000 Mal angesteuert. Unsere Tätigkeitsberichte werden ebenfalls beachtet (ca. 7800 Aufrufe), die Tracking-FAQ gehören zu den beliebtesten Seiten seit ihrer Einrichtung, im vergangenen Jahr waren es über 7000 Aufrufe. Unsere KI-Woche erfreute sich ebenfalls großer Beliebtheit mit über 6000 Aufrufen. Auch die Zahl der Aufrufe von Vorträgen auf PeerTube zeigen uns, dass wir mit unserem Angebot auf Resonanz stoßen.

Unsere Website wird als Informationsquelle genutzt, von verantwortlichen Stellen und von Bürger_innen. Knapp 12.000 Aufrufe verzeichnete allein unser Bürgerreferent. Betrachtet man die signifikant gestiegenen Beschwerdezahlen und die Datenpannenmeldungen so ist erkennbar, dass Datenschutz kein Spezialthema ist, sondern seinen Platz in der Mitte der Gesellschaft hat.

Folgen Sie uns auf Mastodon und PeerTube

Aktuelles vom Datenschutz
und der Informationsfreiheit gibt es auf
den Social Media Kanälen des LfDI

mastodon

bawü.social/@lfdi
bawü.social/@lfdi_pressestelle

PeerTube

tube.bawü.social/a/lfdi_pressestelle

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Kapitel 5

Einzelfälle aus den Abteilungen

5. Einzelfälle aus den Abteilungen

Die Dienststelle lebt von der Fachlichkeit der Abteilungen. Hier bearbeiten wir Einzelfälle und beraten Behörden, Unternehmen, Vereine. Wir führen wo nötig Kontrollen durch. Auch zentrale Dienste werden auf Abteilungsebene erbracht.

5.1. Beauftragte für Chancengleichheit

Im Jahr 2025 knüpfte die Arbeit der Beauftragten für Chancengleichheit (BfC) konsequent an die Erfahrungen und Learnings aus dem Vorjahr an. Die im Jahr 2024 eingeführten niedrigschwelligen Austauschformate hatten sich als äußerst wertvoll erwiesen – sowohl für die Belegschaft als auch für die BfC selbst. Insbesondere die erhöhte Sichtbarkeit der BfC sowie der gezielte Abbau von Hemmschwellen zur Kontaktaufnahme stellten sich als zentrale Erfolgsfaktoren heraus. Gleichzeitig zeigte sich, dass diese Formate es der Belegschaft ermöglichen, eigene Ideen, Anliegen und Bedarfe unmittelbar einzubringen. Die hohe Beteiligung sowie die Qualität der Ergebnisse waren deutlich höher, da Betroffene selbst zu Wort kommen konnten und Themen – wie beispielsweise konkrete Schulungswünsche – direkt aus der Belegschaft heraus formuliert wurden. Auf dieser Grundlage wurden die bestehenden Angebote 2025 fortgeführt, weiterentwickelt und um zusätzliche Formate ergänzt.

Ein zentrales Element war dabei das BfCafé, das im Jahr 2025 in sein zweites Jahr ging. Ziel dieses Formats ist es, Mitarbeitende in informeller Atmosphäre bei Kaffee oder Tee zum Austausch über unterschiedliche Themen einzuladen und den direkten Kontakt zur BfC zu ermöglichen.

Das BfCafé trägt zur Verkürzung von Dienstwegen bei, erhöht die Sichtbarkeit der BfC und dient der systematischen Sammlung von Anregungen, Wünschen und Bedarfen aus der Belegschaft. Diese Rückmeldungen fließen unmittelbar in die weitere Arbeit der BfC ein. Im Berichtsjahr fanden zwei reguläre Termine statt sowie eine Sonderedition in Form eines Elterncafés. Dieses wurde auf ausdrücklichen Wunsch der Belegschaft in einem geschützteren Rahmen durchgeführt und richtete sich an alle Mitarbeitenden, die Eltern sind, bereits länger Eltern sind oder es werden möchten. Die Resonanz der Teilnehmenden war durchweg sehr positiv, sodass eine Wiederholung dieses Formats ausdrücklich gewünscht ist.

Ein weiterer Schwerpunkt lag auf dem Angebot einer Schulung zum Thema „Work-Life-Balance“. Auch dieses Format entstand aus einem konkreten Wunsch der Belegschaft und wurde als halbtägige Veranstaltung umgesetzt. Die Rückmeldungen der Teilnehmenden waren sehr positiv; vielfach wurde berichtet, dass die Inhalte als hilfreich und unterstützend für den eigenen Arbeits- und Lebensalltag empfunden wurden.

Darüber hinaus wurde im Jahr 2025 ein Neulings- bzw. Rückkehrendenkaffee als weiteres niedrigschwelliges Austauschformat eingerichtet. Neue Mitarbeitende sowie Rückkehrer_innen aus z. B. Elternzeit werden nach einigen Monaten gezielt angesprochen und zu einem etwa 30-minütigen Treffen bei Kaffee oder Tee eingeladen. Das freiwillige Angebot ist bewusst ohne feste Agenda oder Zielsetzung gestaltet und dient ausschließlich dem gegenseitigen Kennenlernen sowie dem Aufbau einer künftigen niederschwelligen Kontaktaufnahme zur BfC bei Bedarf oder Wunsch. Dieses Format erwies sich als besonders wertvoll und bestätigte die positiven Erfahrungen aus anderen Sichtbarkeits- und Austauschmaßnahmen.

Durch diese persönlichen Gespräche konnte die BfC deutlich zielgerichteter wahrnehmen, welche Themen,

Bild: Jamillah Knowles & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Anliegen und Bedarfe in der Belegschaft bestehen – Informationen, die auf anderem Wege häufig nicht sichtbar geworden wären. Außerdem konnte auch Vertrauen aufgebaut werden – eine wichtige Grundlage.

Aufgrund des Umzugs der Dienststelle konnte die BfC-Bibliothek im Jahr 2025 nicht weiter ausgebaut werden. Sie wird jedoch weiterhin gepflegt und fortgeführt.

Neben den dienststelleninternen Aktivitäten engagierte sich die BfC auch 2025 ressortübergreifend im Arbeitskreis Chancengleichheit gemeinsam mit anderen Ministerien. In diesem Rahmen wurden Thementage zur Chancengleichheit organisiert. Der Auftakt fand in Präsenz im Haus der Wirtschaft statt, weitere Veranstaltungen wurden online durchgeführt. Die Thementage standen unter dem Titel „Stronger Together – Frauen vernetzen, Zukunft gestalten“ und wurden dankenswerterweise mit finanzieller Unterstützung des Sozialministeriums realisiert. Die BfC des LfDI war ebenfalls unter anderem an der Mitorganisation beteiligt, beispielsweise bei der Erstellung von Flyern im Landesdesign. Die Auftaktveranstaltung verzeichnete rund 500 Teilnehmende. Zu Beginn sprach Staatssekretärin im Ministerium für Soziales, Gesundheit und Integration Dr. Ute Leidig Grußworte. Inhaltlich umfassten die Thementage unter anderem ein Self-Empowerment-Angebot unter dem Motto „Ich zeige mich. Ich wirke. Ich gehe los.“, Veranstaltungen zur Altersvorsorge bei unterbrochener Erwerbstätigkeit oder Teilzeit, zum Vermögensaufbau mit Aktien, ETFs und vergleichbaren Anlageformen sowie zur Gewaltprävention. Wegen der positiven Resonanz werden einzelne Online-Veranstaltungen auch im Jahr 2026 erneut angeboten.

Für das Jahr 2026 ist geplant, die bewährten Formate wie das BfCafé, das Elterncafé, thematische Schulungen sowie die Einzelkaffeetermine fortzuführen. Trotz der zusätzlichen Belastungen durch den fordernden Vorsitz der DSK sollen diese Angebote beibehalten werden, da die positiven Erfahrungen, die hohe Beteiligung und der unmittelbare Mehrwert für die Belegschaft und die BfC selbst deren Bedeutung deutlich unterstreichen.

5.2. Abteilung 1: Zentraler Service

Unser Zentraler Service ist das organisatorische Rückgrat der Dienststelle, verwaltet unseren Haushalt und macht das Personalmanagement.

Einen Schwerpunkt im Sachgebiet Organisation bildete die Verlegung des Behördensitzes. Da der Mietvertrag für das bisherige Dienstgebäude in der Lautenschlagerstraße 20, 70173 Stuttgart, nicht über den 31. Mai 2026 hinaus verlängert werden konnte, haben wir in enger und guter Zusammenarbeit mit dem Landesbetrieb Vermögen und Bau Baden-Württemberg (VB BW), Amt Stuttgart, einen neuen Standort für die Dienststelle gefunden. Das neue Dienstgebäude in der Heilbronner Straße 35, 70191 Stuttgart, liegt zentral in unmittelbarer Nachbarschaft des Europaviertels, nur wenige Gehminuten vom Hauptbahnhof und der U-Bahnstation Stadtbibliothek entfernt, was für die Zugänglichkeit der Dienststelle sehr wichtig ist. Nach Abschluss eines entsprechenden Mietvertrags konnte der Umzug kurz vor Weihnachten 2025 vollzogen worden. Hiermit wurde auch eine wesentliche Voraussetzung geschaffen, um die mit dem baden-württembergischen Vorsitz in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) im Jahr 2026 verbundenen Herausforderungen bewältigen zu können.

Im Zuge des Umzugs haben wir – auch vor dem Hintergrund der veränderten Ressourcensituation – personelle Veränderungen zum Anlass genommen, aufbauorganisatorische Anpassungen vorzunehmen. Die bislang als Stabsstelle bei der Dienststellenleitung angesiedelte Bildungszentrum für Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB) wurde in die Abteilung 6 (Informationsfreiheit) integriert, so dass diese nun aus zwei Sachgebieten (Informationsfreiheit und BIDIB) besteht. Der bisherige Aufgabenzuschnitt des BIDIB und sein Leistungsangebot bleiben hierdurch weitestgehend unberührt.

Im Bereich Arbeitsschutz haben wir zudem im Jahr 2025 die psychischen Gefährdungsbeurteilung in Zusammenarbeit mit einem externen Dienstleister für Angelegenheiten der betriebsärztlichen Betreuung und der Arbeitssicherheit durchgeführt. An der internen Steuerungsgruppe für diese Maßnahme wirken neben dem Sachgebiet Organisation auch der Personalrat und die Beauftragte für Chancengleichheit mit. Die für psychische Gefährdungsbeurteilung benötigten zusätzlichen Mittel, die fixen Ausgaben für gesetzlich vorgegebene Maßnahmen im Bereich Arbeitsmedizin und Arbeitssicherheit und die angespannte Haushaltssituation haben es erforderlich gemacht, die Finanzierbarkeit weiterer Maßnahmen kritisch zu hinterfragen. In diesem Zusammenhang mussten wir uns dazu entschließen, das seit Corona-Zeiten angebotene Employee Assistance Program (EAP) zur psychosozialen Individualberatung zum Jahresende 2025 zunächst auslaufen zu lassen.

Im Bereich des Personalmanagements waren im Jahr 2025 Abgänge von mehreren langjährig bei uns Beschäftigten, insbesondere in zentralen Funktionen, zu verzeichnen. Alle Stellen konnten jedoch noch im gleichen Jahr nachbesetzt werden. Die Abordnung eines unserer Referenten an unsere Dienststelle für den Bereich Datenschutz im Schulbereich konnte im Jahr 2025 für mehrere Jahre verlängert werden. Hierfür danken wir dem Kultusministerium sehr, insbesondere angesichts des Wegfalls der drei Projektstellen für SchuleDigital. Weiterhin konnte die Regelbeurteilungsrunde 2024 im Jahr 2025 abgeschlossen werden. Die hieraus resultierenden Personalentwicklungsmaßnahmen konnten ebenfalls noch im Jahr 2025 vollzogen werden.

Im Sachgebiet Personal wurde zudem der Chancengleichheitsplan in enger Abstimmung mit der Dienststellenleitung und der Beauftragten für Chancengleichheit fortgeschrieben. Nach erfolgter Zustimmung des Personalrats ist der neue Plan zum 1. Januar 2026 in Kraft getreten und gilt bis Ende 2031.

Aufgrund einer weiter erhöhten Zahl an Beschäftigten mit Schwerbehinderung ist in der Dienststelle eine gesonderte Schwerbehindertenvertretung nach § 177 Neuntes Buch Sozialgesetzbuch (SGB IX) einzurichten. Die erstmalige Wahl der Schwerbehindertenvertretung wurde 2025 über den Personalrat in die Wege geleitet.

5.3. Abteilung 2: Inneres, Videoüberwachung und Verkehr

In dieser Abteilung bündeln wir alle Fragen des Kommunalen und der Landesbehörden. Hier sind auch unsere Verkehrsexpert_innen aktiv und nicht zuletzt befassen sich unsere Kolleg_innen mit dem im Jahr 2025 viel diskutierten Thema Videoüberwachung.

5.3.1. Datenschutz frühzeitig mitdenken

Art. 57 Abs.1 Buchst. c) DS-GVO

Wir hören in der Diskussion um Entbürokratisierung immer wieder: Datenschutz sei Bürokratie, Datenschutz verhindere. Abgesehen davon, dass „Bürokratie“ bei hoheitlichem Handeln wichtige rechtsstaatliche Funktionen erfüllt, z. B. die Nachvollzieh- und Vergleichbarkeit von Entscheidungen sicherstellt, gibt es viele Möglichkeiten, Arbeitsaufwand bei öffentlichen Stellen beim Thema Datenschutz zu reduzieren. Denn für alle öffentlichen Stellen gilt: ihre Herausforderungen und Aufgaben sind gleich oder sehr vergleichbar, auch wenn sie aus verfassungsrechtlichen Gründen eigenständig sind.

Bereits in unserem vergangenen Tätigkeitsbericht haben wir das für die Kommunen aufgegriffen und auf die Vorteile der Vernetzung und des Wissensaustauschs untereinander verwiesen. Es ist nicht unsere Aufgabe, die Fachverfahren in den Städten und Gemeinden zu vereinheitlichen, auch steht es uns nicht zu, Gesetzestexte klarer zu formulieren – wir beraten lediglich dazu. Wir meinen, klar definierte, sauber durchdeklinierte digitale Prozesse und einheitliche technische Verfahren würden extrem dabei helfen, Bürokratie zu reduzieren. Dies würde sogar dabei helfen, dass Bürger_innen klarer staatliches Handeln nachvollziehen können. Es würde auch dabei helfen, dass Datenschutz einheitlich umgesetzt würde. Effiziente Prozesse könnten z. B. den Einsatz von Auftragsverarbeitern oder die Nutzung gleicher IT-Infrastruktur zwischen den öffentlichen Stellen erleichtern: die Informationen selbst verbleiben in der Hoheit der zuständigen Stellen, aber die Umsetzung der Verarbeitungsprozesse wird mit ihnen weniger aufwendig.

Eine Erleichterung dieser Art ist beispielsweise mit dem aktuellen Gesetzentwurf zur Änderung des Landesdatenschutzgesetzes (LDSG-E) geplant: § 7a LDSG-E enthält eine Möglichkeit für die Landesregierung (Teile von) Auftragsverarbeitungsvereinbarungen für nachgeordnete Stellen durch Rechtsverordnung zu regeln. Dadurch können Einzelvereinbarungen entfallen oder erheblich an Umfang verlieren.

Nicht nur in der Kommunalverwaltung stellen sich diese Fragen. Auch bei anderen öffentlichen Stellen, wie etwa der Polizei könnten Synergieeffekte besser genützt werden, z. B. durch klare verwaltungsinterne Prozesse und Vereinbarungen oder auch durch eine gesetzliche Klarstellung. Es gilt daher: binden Sie uns frühzeitig ein.

Effizienter und wirksamer Datenschutz ist möglich, auch im Sog der digitalen Entwicklung. Bild: Sophie Valeix & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Digitale Parkraumüberwachung

Ein Beispiel, wie Datenschutz by Design durch frühzeitige Einbindung gelingen kann, möchten wir hier benennen: Parkraumüberwachung mittels Scanfahrzeugen.

Wie lief die Beratung? Da es sich bei der Parkraumkontrolle mit Scanfahrzeugen um eine Überwachung des öffentlichen Raumes handelt, bedurfte es einer tragfähigen gesetzlichen Grundlage. Wir waren daher zunächst im Rahmen des Gesetzgebungsverfahrens für das Landesmobilitätsgesetzes (LMG) beteiligt worden und haben bereits zu diesem Zeitpunkt die geplanten Rechtsgrundlagen für den Einsatz von Scanfahrzeugen datenschutzrechtlich erstmalig bewertet.

Datenschutzrechtlich war unter anderem wichtig, dass klare Regelungen über das konkrete Verfahren getroffen wurden. Das heißt, wie genau und zu welchen Zwecken welche personenbezogenen Daten, hier insbesondere Kennzeichen, erhoben bzw. erfasst, weiterverarbeitet und gelöscht werden. Hierbei waren auch Regelungen für die Fälle zu schaffen, in denen eine Parkberechtigung vorliegt und die erhobenen personenbezogenen Daten unverzüglich gelöscht werden müssen, da eine weitere Verarbeitung und Speicherung der Daten hier nicht erforderlich sind.

Neben den Regelungen zur Datenverarbeitung im Zusammenhang mit dem Abgleichvorgang, musste auch die Verarbeitung personenbezogener Daten von Personen, die sich zufällig im Bildbereich befinden, geregelt werden, da deren Datenverarbeitung für die Feststellung des Parkverstoßes ebenfalls nicht erforderlich ist. Sie sind daher unkenntlich zu machen. Darüber hinaus ist möglichst transparent zu machen, dass mit den Scanfahrzeugen eine Datenverarbeitung in der Form einer digitalen Parkraumkontrolle erfolgt.

Infokasten

„Wissen vernetzen: datenschutzreche Beratung für öffentliche Stellen“, LfDI BW, 40. Tätigkeitsbericht Datenschutz 2024, S. 93f.: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2025/03/TB_40_Datenschutz-2024_barrierefrei.pdf

Im März 2025 hat der Landesgesetzgeber mit § 13 LMG dann die entsprechende Rechtsgrundlage für die Datenerhebung und -verarbeitung zum Zweck der digitalen Parkraumkontrolle beschlossen. Nach Beschluss des Gesetzes wurden wir vom Verkehrsministerium Baden-Württemberg konsultiert und haben in Bezug auf die Ausgestaltung der Datenverarbeitung durch die Scanfahrzeuge datenschutzrechtlich Stellung genommen und das Ministerium beraten.

Das Verkehrsministerium hat uns die geplante technische Umsetzung der Scanfahrzeuge vorgestellt und näher erläutert. Im Rahmen dieser Erörterung wurden von uns noch einige Verbesserungsvorschläge eingebracht (u.a. zum Löschkonzept). Auch nach diesem Auftaktgespräch standen wir regelmäßig in Kontakt mit dem Verkehrsministerium, um rechtliche Fragen zum Datenschutz der technischen Umsetzung zu thematisieren und Lösungen für auftretende Probleme zu erarbeiten.

Die Zusammenarbeit ist sehr konstruktiv. Wir begleiten das Projekt auch weiterhin und bedanken uns an dieser Stelle bei dem Verkehrsministerium für die bisherige gute Zusammenarbeit.

5.3.2. Digitalisierung der Verwaltung

Datenschutz als Rückenwind – wie gute Regeln die Verwaltungsdigitalisierung möglich machen

Die Digitalisierung der Verwaltung steht seit Jahren unter hohem Erwartungsdruck: Leistungen sollen schneller, einfacher und medienbruchfrei bereitgestellt werden. Gleichzeitig wachsen die Anforderungen an IT-

Infokasten

Orientierungshilfe der DSK zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG): https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG_Version_1_1.pdf

Den Prüfprozess finden Sie unter: https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Standardisierter_Pruefprozess_OZG.pdf

Sicherheit, Datenschutz und Transparenz. Datenschutz wird dabei noch immer zu häufig als Hemmnis wahrgenommen. Die Erfahrung zeigt jedoch: Gerade bei komplexen Digitalisierungsprojekten ist Datenschutz kein Gegner, sondern die Voraussetzung für tragfähige, vertrauenswürdige Lösungen.

Gestalten, begleiten, möglich machen

Im Jahr 2025 lag der Schwerpunkt unserer Arbeit darauf, Datenschutz als gestaltendes Element der Verwaltungsdigitalisierung sichtbar und nutzbar zu machen.

Ein zentrales Ergebnis unserer Mitarbeit in der OZG 2.0-Kontaktgruppe der Datenschutzkonferenz (DSK) war die Überarbeitung der Anwendungshilfe „Ausgewählte Fragestellungen des neuen Onlinezugangsgesetzes – Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen – Version 1.1“. Ziel war es, rechtliche Anforderungen für Onlinedienste nach §§ 2 Abs. 8, 8a OZG noch verständlicher aufzubereiten und den datenschutzrechtlich Verantwortlichen eine klare, praxisnahe Grundlage für die Konzeption und den Betrieb von Onlinediensten an die Hand zu geben.

Dabei wurde die Orientierungshilfe aus 2024 um Ausführungen, wann es sich um einen länderübergreifenden Onlinedienst i.S.v. § 2 Abs. 8 OZG handelt, ergänzt. Es wurde erläutert, wann dem § 8a Abs. 4 OZG entgegenstehende datenschutzrechtliche Vereinbarungen aufgehoben werden müssen und Ergänzungen zum Nutzerkonto aufgenommen.

Darauf aufbauend haben wir zusammen mit anderen Datenschutzaufsichtsbehörden in der OZG 2.0 -Kontaktgruppe einen „Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onli-

Weitere Informationen

https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html

FITKO: Föderale IT-Kooperation: Der IT-Planungsrat hat eine agile Organisation geschaffen, um die Digitalisierung der öffentlichen Verwaltung zielgerichtet zu koordinieren und gemeinsam mit Bund, Ländern und Kommunen effektiv voranzutreiben. Damit sollen innovative digitale Lösungen für eine moderne, wirksame und resiliente Verwaltung in Deutschland realisiert werden. (Webseite: https://www.fitko.de/)

EfA-Prinzip und EfA-Onlinedienste: Die Umsetzung des Onlinezugangsgesetz (OZG) stellt ein sehr großes Modernisierungsvorhaben der öffentlichen Verwaltung dar. Mit dem „Einer für Alle“ (EfA)-Prinzip wurde in Zusammenhang mit dem OZG eine nachhaltige, arbeitsteilige Arbeitsstruktur für die interföderale Zusammenarbeit geschaffen. Das EfA-Prinzip bildet die Grundlage für die Nachnutzung von digitalisierten Leistungen: Jedes Land sollte Leistungen so digitalisieren, dass andere Länder diese nachnutzen können und den Onlinedienst nicht nochmal selbst entwickeln müssen. Das spart Zeit, Ressourcen und Kosten. Der Grundgedanke hinter EfA ist, dass Bund, Länder und Kommunen nicht jedes digitale Verwaltungsangebot eigenständig neu entwickeln müssen, sondern durch effiziente Arbeitsteilung von den Digitalisierungsvorhaben anderer profitieren.

Abkürzungen:
EfA = Eine für Alle
EGovG BW = Gesetz zur Förderung der elektronischen Verwaltung des Landes Baden-Württemberg
FITKO = Föderalen IT-Kooperation
LBO = Landesbauordnung für Baden-Württemberg
NOOTS-Staatsvertrag = Gesetz zum Vertrag über die Errichtung, den Betrieb und die Weiterentwicklung des Nationalen Once-Only-Technical-Systems (NOOTS) – Vertrag zur Ausführung von Art. 91c Abs. 1, Abs. 2 GG – NOOTS-Staatsvertrag
OZG = Onlinezugangsgesetz

nediensten nach Onlinezugangsgesetz (OZG)“ erstellt. Der Leitfaden soll Projektverantwortliche dabei unterstützen, Datenschutz systematisch und frühzeitig bei Digitalisierungsvorhaben zu integrieren. Er zeigt auf, wie Verantwortlichen gemäß § 8a OZG einen standardisierten Prüfprozess gestalten können und eine Datenschutzkonformität der jeweils entwickelten OZG-Dienste sichergestellt werden kann. Zugleich soll damit ein einheitlicher und transparenter Standard im Hinblick auf die Datenschutzprüfung von EfA-Onlinediensten nach OZG etabliert werden.

Flankiert wurde unsere konzeptionelle Arbeit von einem intensiven fachlichen Austausch mit Vertretenden einzelner Kompetenzteams des IT-Planungsrats, der FITKO, unterschiedlichen Ministerien in Baden-Württemberg und registerführenden Stellen des Landes. In verschiedenen Gesprächsformaten konnten wir datenschutzrechtliche Perspektiven in laufende Entwicklungen einbringen und zugleich wertvolle Einblicke in technische und organisatorische Herausforderungen gewinnen. Die Dialoge auf Augenhöhe haben gezeigt, wie wichtig frühzeitige Abstimmungen für den Erfolg föderaler Digitalprojekte sein können.

Darüber hinaus haben wir im Berichtsjahr eine Vielzahl von Stellungnahmen zu Gesetzesvorhaben und -änderungen zu unterschiedlichen Digitalisierungs- und Verwaltungsvorhaben verfasst (z. B. NOOTS-Staatsvertrag, Änderung des EGovG BW, Änderung der LBO). Dabei war es unser Anspruch, Datenschutz nicht abstrakt, sondern lösungsorientiert zu adressieren und konkrete Hinweise für eine rechtssichere Ausgestaltung zu geben. Ergänzend dazu haben wir einzelne Landesprojekte begleitet.

Das Jahr 2025 hat eindrucksvoll gezeigt: Datenschutz entfaltet seine größte Wirkung, wenn er frühzeitig, praxisnah und dialogorientiert eingebunden wird. Orientierungshilfen, Leitfäden und kontinuierlicher Austausch schaffen Vertrauen, beschleunigen Entscheidungsprozesse und erhöhen die Qualität digitaler Verwaltungsleistungen. Für die kommenden Jahre empfiehlt es sich, Datenschutz weiterhin als festen Bestandteil von Projektmanagement bei öffentlichen Digitalisierungsvorgaben, der entsprechenden Gesetzgebung und IT-Architektur zu verankern. Wer Datenschutz als Ermöglicher versteht, schafft nicht nur rechtssichere, sondern auch nachhaltige und bürgerfreundliche digitale Verwaltung.

5.3.3. Ein bunter Strauß aus der Videoüberwachung

Art. 57 Abs.1 Buchst. a), c), d), f) DS-GVO

Die Videoüberwachung entwickelte sich im vergangenen Jahr zu einem der dynamischsten Themen unserer aufsichtsrechtlichen Tätigkeit. Einerseits wird vehement eine Ausweitung von Videoüberwachung im öffentlichen Raum gefordert, andererseits ist die Anzahl der Beratungsanfragen und Beschwerden zu Videoüberwachungen gegenüber den Vorjahren erheblich gestiegen. Dieser deutliche Zuwachs betraf sowohl den öffentlichen als auch den nicht-öffentlichen Bereich und führte zu einer spürbaren Verdichtung der aufsichtsbehördlichen Arbeit.

So stieg die Anzahl der neueingegangenen Beschwerden über Videoüberwachungskameras und Hinweise hierzu von 442 Fällen im Jahr 2024 auf 800 Fälle im Jahr 2025 – eine Steigerung von rund 80 %.

Beratung, Zuständigkeiten und rechtliche Grenzen

Als Rechtsgrundlage für die Videoüberwachung durch öffentliche Stellen kommen je nach den örtlichen Gegebenheiten in der Regel das Polizeigesetz (PolG) oder die DS-GVO i. V. m. dem Landesdatenschutzgesetz (LDSG) in Betracht.

Gemäß Art. 6 Abs.1 Buchst. e) DS-GVO i. V. m. § 18 LDSG ist die Beobachtung öffentlich zugänglicher Räume mithilfe optisch-elektronischer Einrichtungen zulässig, soweit dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen zu schützen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. § 18 LDSG gilt gemäß § 2 LDSG für Behörden und sonstige Stellen des Landes, der

Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen).

Im öffentlichen Bereich erreichten uns vorrangig Beratungsanfragen von Kommunen. Im Mittelpunkt stand regelmäßig die Frage, unter welchen Voraussetzungen Videoüberwachung durch kommunale Stellen zulässig ist und wie diese von polizeilichen Befugnissen nach dem Polizeirecht abzugrenzen ist.

Einsatz von Videoüberwachung an Schulen

Ein wiederkehrender Beratungsschwerpunkt betraf die Videoüberwachung an Schulen. In der Praxis zeigte sich häufig eine unklare Zuständigkeitsverteilung zwischen dem kommunalen Schulträger (regelmäßig der Kommune) und der Schulleitung. Während die Schulträger für Gebäude und Liegenschaften verantwortlich sind, liegt die pädagogische und organisatorische Verantwortung bei der Schulleitung. Diese Überschneidung führt in der Praxis zu Unsicherheiten hinsichtlich der datenschutzrechtlichen Verantwortlichkeit, der Entscheidungsbefugnis über den Einsatz von Videoüberwachungstechnik sowie der Frage, auf welcher Rechtsgrundlage eine solche Maßnahme überhaupt erfolgen kann. Wir stellten im vergangenen Berichtszeitraum wiederholt klar, dass Videoüberwachung an Schulen nur unter besonders engen Voraussetzungen zulässig ist.

Schulen sind Schutzräume für Kinder und Jugendliche, weshalb hier erhöhte Anforderungen an die Verhältnismäßigkeit, Transparenz und Zweckbindung der Datenverarbeitung gelten. Eine pauschale Berufung auf Sicherheitsinteressen oder Vandalismusprävention genügt regelmäßig nicht. Zudem wurde darauf hingewiesen, dass schulische Videoüberwachung nicht dazu dienen darf, polizeiliche Aufgaben zu ersetzen oder Verhaltenskontrollen vorzunehmen.

Videoüberwachung von öffentlich zugänglichen Müllcontainerstandorten

Ein weiterer wesentlicher Problembereich war die Videoüberwachung von öffentlich zugänglichen Müllcontainerstandorten. Kommunen beabsichtigen hier häufig, illegale Müllablagerungen zu verhindern. Da sich die Container vielfach im allgemeinen Straßenraum oder in sonstigen öffentlich zugänglichen Bereichen befinden und eine bauliche Abgrenzung fehlt, ist eine datenschutzkonforme Beschränkung des Erfassungsbereichs regelmäßig nicht möglich. In der Folge ist eine Videoüberwachung unter Beachtung der gesetzlichen Vorgaben in diesen Fällen in der Regel unzulässig. Wir wiesen in der Beratung wiederholt darauf hin, dass ordnungsrechtliche Probleme nicht durch flächendeckende Videoüberwachung gelöst werden können und alternative Maßnahmen vorrangig zu prüfen sind.

Videoüberwachung zur Kriminalitätsbekämpfung

Soll mit einer Videoüberwachungsmaßnahme hingegen Kriminalität bekämpft werden, kommt § 44 Abs. 3 PolG als Rechtsgrundlage in Frage. Dieser richtet sich sowohl an den Polizeivollzugsdienst als auch an Ortspolizeibehörden und erlaubt die Überwachung von öffentlichen Orten zur Kriminalitätsbekämpfung. § 44 Abs. 3 PolG kommt jedoch nur bei Straftaten, hingegen nicht bei Ordnungswidrigkeiten in Betracht. Für seine Anwendung müssen kumulativ zwei Voraussetzungen vorliegen:

a. Es muss sich um einen Kriminalitätsschwerpunkt handeln und
b. eine Kriminalitätsprognose muss davon ausgehen, dass voraussichtlich auch künftig Straftaten begangenen werden.

Ein Kriminalitätsschwerpunkt setzt voraus, dass der zu überwachende Ort sich in seiner Kriminalitätsbelastung deutlich vom übrigen Gemeindegebiet abhebt. Einen Orientierungspunkt für die Kriminalitätsbelastung bildet in erster Linie die Straßenkriminalität. Gleichzeitig können auch Betäubungsmitteldelikte betrachtungsrelevant sein.

Bei der Realisierung der Maßnahme gilt es diese möglichst grundrechtsschonend umzusetzen, da die Mehrzahl der überwachten Personen dafür keinen Anlass gegeben hat und sich viele Menschen durch solch eine Überwachung in Ihrer Handlungsfreiheit eingeschränkt sehen. Die Videoüberwachung sollte daher auf Zeiten beschränkt werden, in denen der Großteil der festgestellten Straftaten begangen wird. Auch gilt es darauf zu achten, dass besonders sensible Bereiche wie z. B. Eingänge von Privatwohnhäusern nicht überwacht werden.

Videoüberwachung unter Nachbarn

Ein Großteil der bei uns eingehenden Beschwerden richtet sich gegen die Videoüberwachung in der Nachbarschaft. Die beschwerdeführenden Personen tragen hier regelmäßig vor, dass Nachbarn über ihre Grundstücke hinaus fremde Grundstücke oder auch die Straße aufnehmen würden. Um den Beschwerdeführenden eine erste Orientierung zu bieten, haben wir ein Hinweisblatt namens „Erste Hilfe bei Videoüberwachung in der Nachbarschaft“ erstellt. In dieser werden mittels kurzer Fragen die Voraussetzungen einer zulässigen Videoüberwachung dargestellt und Hinweise gegeben, wie mit dem Verdacht einer möglichen unzulässigen Videoüberwachung eines Nachbarn umgegangen werden kann. Ausführlichere Informationen zur Videoüberwachung durch Privatpersonen und Unternehmen im Allgemeinen sind auch weiterhin in der Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ der Datenschutzkonferenz (DSK) zu finden.

Videoüberwachung in der Gastronomie

Ein ebenfalls häufig wiederkehrender Fall ist die Videoüberwachung in Gaststättenbetrieben. Hier werden regelmäßig neben dem Gastraum auch die Arbeitsplätze der Mitarbeiter erfasst. Sei es hinter der Theke oder auch in der Küche.

Ein besonders drastischer Fall wurde Ende 2023 an uns herangetragen. Vorgetragen wurde hier, die Inhaberin eines Gastronomiebetriebes überwache sowohl den Gastraum als auch die Küche. Dabei beschränke sich die Überwachung nicht allein auf die Aufnahme und Speicherung von Bilddaten, sondern es würden auch Tonaufnahmen gefertigt werden.

Aufgrund der nach einer Rückfrage erfolgten Glaubhaftmachung der Vorwürfe durch die beschwerdeführende Person, führten wir bereits kurze Zeit später eine unangekündigte Kontrolle in dem Gastronomiebetieb durch.

Dabei konnten wir zwei Kameras feststellen, wovon eine die Theke, den Gastraum sowie den öffentlichen Bereich erfasste und eine die Küche. Es erfolgte eine durchgehende Liveübertragung und eine Speicherung der Bilddateien bei erkannter Bewegung.

Auf Nachfrage, ob auch Tonaufzeichnungen gefertigt würden, wurde uns von der Inhaberin mitgeteilt, dass sie glaube, dass dies nicht der Fall sei. Bei der Sichtung der gespeicherten Aufnahmen konnte jedoch festgestellt werden, dass die Aufnahmen auch Tonaufzeichnungen enthielten und einen Monat gespeichert worden sind.

Neben der datenschutzrechtlichen Relevanz können Tonaufnahmen auch strafrechtliche Relevanz haben. Nach § 201 Strafgesetzbuch ist die unbefugte Aufnahme des nichtöffentlich gesprochenen Wortes strafbar.

Auch fehlten entsprechende Hinweisschilder, die die Besuchenden über die Videoüberwachung informieren.

Noch vor Ort wurde der Inhaberin mitgeteilt, dass die Tonaufzeichnungen zu unterlassen, die Videoaufnahmen zu löschen, Hinweisschilder anzubringen und die Kameras während der Arbeits- und Öffnungszeiten auszuschalten sind. In der vor Ort festgestellten Einstellung der Kameras war der Betrieb während diesen Zeiten nicht zulässig.

Zum Einbruchs- und Diebstahlsschutz kann eine Videoüberwachung außerhalb der Zeiträume, in denen der Betrieb für den Kundenverkehr geöffnet ist bzw. Beschäftigte ihrer Arbeit nachgehen (also während der Öffnungs- und Arbeitszeiten) erfolgen. Durch zum Beispiel das manuelle Ein- und Ausschalten der Kameras, den Einsatz einer Zeitschaltuhr oder einer entsprechenden Programmierung der Kamera kann sichergestellt werden, dass die Videoüberwachung nur außerhalb der Öffnungs- und Arbeitszeiten stattfindet. Im Anschluss an den Kontrolltermine erging eine gebührenpflichtige Verwarnung an die Inhaberin.

Videoüberwachung in Schwimmbädern

Regelmäßig erreichen uns auch Eingaben von Schwimmbadbesucher_innen, die bei ihrem Aufenthalt im Schwimmbad Videokameras entdeckt haben. Für Schwimmbadbetreibende gibt es bereits seit 2019 eine Orientierungshilfe der DSK zur Videoüberwachung in Schwimmbädern. In dieser wird die Videoüberwachung der typischen Schwimmbadbereiche beleuchtet.

So kann es Bereiche geben, in denen eine solche zulässig ist wie beispielsweise in Schwimmbereichen mit erhöhter Gefährlichkeit wie bei Rutschen oder Sprungtürmen. Hier kann ein Live-Monitoring (ohne Speicherung) als verlängertes Auge der Bademeister_innen zulässig sein. Auf diese Weise können Bademeister_innen über Monitore mehrere Bereiche zeitgleich im Auge behalten. Dabei darf die Videobeobachtung jedoch nie als Ersatz für die Aufsicht durch Personal dienen.

Umkleidekabinen, Umkleidebereiche, aber auch der Vorbereich vor Umkleiden dürfen hingegen grundsätzlich nicht überwacht werden. Problematisch ist dies in der Praxis häufig, wenn sich in diesen Umkleidebereichen bzw. dem Vorbereich der Umkleide auch Spinde für die Gäste befinden. Diese werden aufgrund befürchteter Aufbrüche häufig videoüberwacht. Dabei wird jedoch nicht bedacht, dass zeitgleich der Vorbereich der Umkleidekabinen erfasst wird. Vor der Installation von Videokameras sollte daher eine genaue Prüfung erfolgen, welche Bereiche die Kameras (mit-)erfassen und auch, ob es mildere Mittel gibt, wie zum Beispiel das Angebot von Wertschließfächern, die getrennt von den Umkleidebereichen angebracht werden können. Diese dürften dann aufgrund der erhöhten Gefährdungslage (Aufbrüche und Diebstahl) videoüberwacht werden.

Infokasten

Hinweisblatt „Erste Hilfe bei Videoüberwachung in der Nachbarschaft": https://www.baden-wuerttemberg.datenschutz.de/erste-hilfe-bei-videoueberwachung-in-der-nachbarschaft/

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/09/20200903_oh_vue.pdf

Neben der rechtlichen Prüfung nahmen wir in allen Bereichen der Videoüberwachung auch eine vermittelnde und beratende Rolle ein. In vielen Fällen konnten durch Anpassungen der Kameratechnik, Einschränkung des Erfassungsbereichs oder organisatorische Maßnahmen einvernehmliche Lösungen erzielt werden.

Änderung des LDSG im Hinblick auf die Videoüberwachung

Im September 2025 erfolgte die offizielle Beteiligung unseres Hauses im Rahmen des Gesetzgebungsverfahrens. Wir haben eine umfangreiche datenschutzrechtliche Stellungnahme abgegeben. Aus unserer Sicht gab es insbesondere im Hinblick auf die Videoüberwachung noch zahlreichen Klärungsbedarf, auf den wir hingewiesen haben.

Nach erfolgter Rückmeldung der im Gesetzgebungsverfahren zu beteiligenden Stellen, wurde eine finale Änderungsentwurf erstellt, die im Dezember in erster Lesung in den Landtag eingebracht wurde.

Neben der sprachlichen Überraschung, dass § 18 künftig mit „Videoschutz“ statt „Videoüberwachung“ überschrieben werden soll (der Gesetzestext in § 18 selbst sowie §§ 18a, 18b beinhalten hingegen weiterhin den Begriff „Videoüberwachung“ bzw. „Überwachung“), finden sich zahlreiche Unklarheiten, teils auch verfassungsrechtlicher Natur. Es soll sich im Folgenden nur auf die besonders gravierenden Bereiche beschränkt werden.

Der im Vergleich mit anderen Bundesländern derzeit recht eingeschränkte Anwendungsbereich der Videoüberwachung soll durch den neuen § 18 Abs.1 LDSG-E umfangreich erweitert werden. Bislang sah Abs.1 eine Reihe von Objekten vor, in und bei denen eine Videoüberwachung zulässig ist.

Steht der Wegfall dieser Einschränkungen noch im Ermessen des Gesetzgebers, so dürfte die Angemessenheitsfiktion in § 18 Abs.1 S.3 jedoch sowohl verfassungs- als auch europarechtswidrig sein. Diese sieht vor, dass zum Schutz von „sicherheitsrelevanten Einrichtungen, Dienstgebäuden, Dienstfahrzeugen, Kulturgütern oder öffentlichen Verkehrsmitteln und den dort oder in unmittelbarer Nähe jeweils befindlichen Personen und Sachen“ keine Verhältnismäßigkeitsprüfung mehr durchgeführt werden muss. Die Grundrechte der potentiell von der Videoüberwachung betroffenen Personen fänden keinen Platz mehr. Diese müssten pauschal immer zurücktreten.

Dies widerspricht nicht nur dem Rechtsstaatsprinzip aus Art. 20 Abs. 3 Grundgesetz und Art. 23 Abs.1 der Landesverfassung, sondern auch dem Europarecht (Art. 52 Abs.1 S. 2 Grundrechte-Charta). Diese Normen schreiben eine Verhältnismäßigkeitsprüfung immer dann vor, wenn staatliche Akteure in Grundrechte eingreifen. Dies findet im operativen Teil des geänderten LDSG jedoch keine Beachtung.

Vor dem Hintergrund, dass sich in der Begründung nur Beispiele für die sicherheitsrelevanten Einrichtungen, Dienstgebäude, etc. nach § 18 Abs.1 S.3 LDSG-E finden, wird es zudem der Aufsichtspraxis und ggf. den Gerichten vorbehalten bleiben, festzustellen, welcher Maßstab an diese privilegierten Orte zu stellen sein wird.

Auch die Ausweitung der Speicherung von vier Wochen auf zwei Monate muss kritisch hinterfragt werden. Schon derzeit müssen Videoaufnahmen gelöscht werden, sobald diese nicht mehr notwendig sind für den Zweck, zu dem sie erhoben worden sind (Art. 5 Abs.1 Buchst. e) DS-GVO). Die übliche zulässige Speicherdauer beträgt i.d.R. maximal 72 Stunden. Eine davon

Infokasten

LfDI-Stellungnahme LDSG-E: https://www.baden-wuerttemberg.datenschutz.de/stellungnahme-ldsg/, die Hinweise zur Videoüberwachung, insbesondere S. 41-48).

abweichende Speicherdauer ist nur in Ausnahmefällen zulässig. Sollen die Aufnahmen über die 72 Stunden hinaus gespeichert werden, bedarf es daher einer eigenen Begründung für die längere Speicherdauer, da es sich hierbei um einen selbstständigen, rechtfertigungsbedürftigen Verarbeitungsvorgang handelt. Bereits die derzeitige Regelung führt leider oft zu Missverständnissen hinsichtlich der zulässigen Dauer der Speicherung. So gehen öffentliche Stellen häufig davon aus, dass immer für vier Wochen gespeichert werden dürfe. Mit der Gesetzesänderung ist zu befürchten, dass zukünftig anlasslos Aufnahmen für zwei Monate gespeichert werden.

Es bleibt nun abzuwarten, ob das Gesetz in der Version, die in den Landtag zur ersten Lesung eingebracht wurde, beschlossen wird oder doch noch Änderungen vorgenommen werden. Die parlamentarische Entscheidung findet nach Redaktionsschluss statt.

Ausblick

Die signifikante Zunahme der Vorgangszahlen im Berichtszeitraum unterstreichen, dass Videoüberwachung weiterhin eines der konfliktträchtigsten Themenfelder darstellt und aktueller ist denn je.

Zum einen herrscht in vielen Bereichen immer noch Unsicherheit über die Rechtslage, zum anderen scheint die Videoüberwachung in immer mehr Bereichen unseres Lebens Einzug zu halten. Insbesondere im öffentlichen Bereich zeigt sich ein wachsender Bedarf an frühzeitiger, klarer und praxisnaher Beratung.

Vor diesem Hintergrund und der zu erwartenden Änderung des LDSG mit seinen Normen zur Videoüberwachung wollen wir für das Jahr 2026 einen Schwerpunkt im Bereich „Videoüberwachung“ setzen.

Künftig wird es entscheidend sein, Verantwortlichkeiten deutlicher zu klären, rechtliche Abgrenzungen – insbesondere zwischen kommunaler Aufgabe und polizeilicher Befugnisse – weiter zu schärfen und datenschutzkonforme Alternativen stärker in den Fokus zu rücken. Wir werden unsere Aufsichtstätigkeit auch zukünftig mit einem ausgewogenen Ansatz aus Beratung und Kontrolle fortsetzen.

Neben den bereits vorliegenden zahlreichen Orientierungshilfen zum Thema Videoüberwachung, planen wir daher für nächstes Jahr bspw. weitere Schulungen über unser Bildungszentrum.

Infokasten

Orientierungshilfe zur Videoüberwachung in Schwimmbädern (DSK), vom 8. Januar 2019: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/Orientierungshilfe-zur-Video%C3%BCberwachung-in-Schwimmb%C3%A4dern.pdf

Datenfreiheit, Folge 49, Videoüberwachung und VeRA, vom 29. August 2026: https://www.baden-wuerttemberg.datenschutz.de/datenfreiheit-49-videoueberwachung-vera/

„Keber Quarterly. Videoüberwachung – Störgefühl von gestern und neues Normal?“, vom 6. Oktober 2026 https://www.baden-wuerttemberg.datenschutz.de/keber-quarterly-iii-aufzeichnung

Praxishilfen zur Videoüberwachung: https://www.baden-wuerttemberg.datenschutz.de/praxishilfen/#videoueberwachung

5.3.4. Datenpanne? Maßnahmen zur Behebung oder Abmilderung der möglichen Folgen

Art. 57 Abs.1 Buchst. f) DS-GVO

Passiert eine Verletzung des Schutzes personenbezogener Daten, muss die verantwortliche Stelle nicht nur prüfen, wie sie Ähnliches in Zukunft vermeiden kann, sondern auch, ob und wie sie die bereits eingetretene Verletzung und deren möglichen Folgen für die betroffene Person beheben oder abmildern kann. Bei einer Übermittlung von falschen Informationen müssen diese also gegenüber einem Empfänger korrigiert werden.

Im hiesigen Fall beschwerte sich ein Bürger über eine Stadt, die Teile seines Gehalts bei seiner Arbeitgeberin gepfändet hatte, obwohl keine offenen Forderungen der Stadt gegen ihn bestanden. Im Verlauf des Verfahrens stellte sich heraus, dass ein Fehler beim Abruf aus dem Melderegister passiert war: Der Beschwerdeführer war mit einer Person verwechselt worden, die fast den identischen Namen trug. Deswegen war die Arbeitgeberin der falschen Person ermittelt und ihr die Pfändungs- und Einziehungsverfügung zugestellt worden. Nachdem sich der Bürger bei der Stadt beschwert hatte, bemerkte die Stadt das Versehen und teilte der Arbeitgeberin zwar mit, dass sich die Verfügung erledigt habe – allerdings ohne darüber aufzuklären, dass der Bürger keinerlei Anlass für die Pfändung gegeben hatte, sondern diese auf einer Verwechslung beruhte.

Verwaltungsakte, die zur Zahlung einer Geldleistung verpflichten, werden durch Beitreibung vollstreckt, § 13 Abs.1 Landesverwaltungsvollstreckungsgesetz (LVwVG). Die Beitreibung kann auch dadurch erfolgen, dass die Verwaltungsbehörde selbst eine Pfändungsverfügung ausstellt und die dafür erforderlichen Daten ermittelt, hier u.a. das Geburtsdatum und die Arbeitgeberin des Zahlungspflichtigen. Einer Pfändungsverfügung geht in der Regel ein Verstreichenlassen einer Vielzahl an Fristen voraus, u.a. muss der Verwaltungsakt bestandskräftig werden, seine Vollstreckung angedroht und als Teil des Vollstreckungsverfahrens erneut gemahnt worden sein.

Wird die Gehaltsforderung einer Person gepfändet, erhält eine Arbeitgeberin mittelbar Kenntnis davon, dass die betroffene Person mit einer Zahlung im Rückstand ist und mehrere Zahlungsaufforderungen hat verstreichen lassen. Dadurch könnte beispielsweise der (vermeintliche) Rückschluss auf eine Unzuverlässigkeit oder auf Geldsorgen der betroffenen Person gezogen werden – und daraus wiederum soziale Nachteile für die betroffene Person entstehen, gegebenenfalls sogar wirtschaftliche, wenn sich dieser Schluss negativ auf die Bewertung der Arbeitsleistung auswirkt. Unabhängig davon, ob tatsächlich diese, andere oder keine Schlüsse zum Nachteil der betroffenen Person gezogen werden, muss der Verursacher – im hiesigen Fall die Stadt – sich um die Abmilderung oder Behebung möglicher nachteiliger Auswirkungen bemühen, vgl. Art. 33 Abs. 3 Buchst. d) DS-GVO. Deswegen war es wichtig, dem Arbeitgeber mitzuteilen, dass die Pfändung auf einer Verwechslung beruhte. Denn damit wurde mittelbar auch erklärt, dass der Beschwerdeführer nie mit einer Zahlung gegenüber der Stadt im Rückstand war und auch keine Zahlungsaufforderungen hatte verstreichen lassen.

Infolge unserer Nachfrage bei der Stadt stellte sich heraus, dass der behördliche Datenschutzbeauftragte bisher nicht in das Verfahren eingebunden gewesen und es den Sachbearbeitenden nicht aufgefallen war, dass der Arbeitgeberin unseres Beschwerdeführers ein solcher Eindruck entstehen hätte können. Die Klarstellung wurde unverzüglich nachgeholt und die Beschäftigten für die möglichen Folgen der versehentlichen Übermittlung falscher Informationen nochmals sensibilisiert.

Zu den Pflichten infolge einer Verletzung des Schutzes personenbezogener Daten gehört es auch, mögliche nachteilige Auswirkungen dessen für betroffene Personen abzumildern oder zu beheben. Wird beispielsweise versehentlich das Gehalt einer falschen Person gepfändet, muss die Arbeitgeberin darüber informiert werden, dass eine Verwechslung vorlag, um damit möglichen sozialen oder wirtschaftlichen Nachteilen vorzubeugen.

Wir empfehlen allen Verantwortlichen, für den Fall einer Verletzung des Schutzes personenbezogener Daten Prozesse zu entwickeln, die gut in die eigene Organisationsstruktur eingebettet sind, und intern Informationen bereitzustellen, die Beschäftigte im Fall der Fälle zu Rate ziehen können.

5.3.5. Schutz vor Verlust von Daten

Art. 57 Abs.1 Buchst. a) DS-GVO

Oftmals wird Datenschutz im Wesentlichen als Schutz vor Kenntnisnahme Unbefugter verstanden. Er beinhaltet aber auch den Schutz vor Manipulation oder Verlust von personenbezogenen Daten. Dies wird z. B. dann besonders relevant, wenn die Daten für Verwaltungsverfahren benötigt werden und von der verantwortlichen Stelle selbst nicht ersetzt werden können.

Uns wurde im Verlauf des letzten Jahres von einer öffentlichen Stelle eine Datenpanne gemeldet, bei der ein Ausweisdokument und eine Geburtsurkunde im Original nicht mehr aufgefunden werden konnten. Die betroffene Behörde konnte zwar nachvollziehen, dass die Dokumente bei ihr auf der Poststelle angekommen waren, aber auch eine umfassende Suche ließ sie nicht wieder auftauchen. Deshalb nahm die Behörde an, dass die Unterlagen nach Ablauf einer gewissen Aufbewahrungszeit bei der Poststelle vernichtet worden waren, da diese sie keinem Verfahren zuordnen konnte. So bestand zwar eine hohe Wahrscheinlichkeit, dass keine Kenntnisnahme der Dokumente durch Unbefugte erfolgen konnte, für die betroffene Person war nun aber der Ausgang ihres Verwaltungsverfahrens gefährdet. Denn dafür wurden die Originaldokumente als Nachweis benötigt. Auch traf die betroffene Person selbst keinerlei Verantwortung für den Verlust: die Dokumente waren von ihr bei einer anderen Behörde abgegeben worden. Nachdem diese Behörde ihr Verfahren abgeschlossen hatte, hat diese die Dokumente an eine andere Behörde für ein weiteres Verfahren weitergeleitet. Zuletzt waren sie per Post mit Einschreiben an die Stelle geschickt worden, die sie nicht mehr auffinden konnte.

Infolge der Datenpanne hat die Behörde der betroffenen Person eine längere Frist zur Einreichung der erforderlichen Unterlagen eingeräumt, die Kostenübernahme für die Neubeschaffung angeboten und damit die Folgen der Verletzung des Schutzes personenbezogener Daten abgemildert, vgl. Art. 33 Abs. 3 Buchst. d) DS-GVO. Nicht aufgefangen werden konnte durch diese Maßnahmen allerdings, dass hier eine Person

Personenbezogene Daten werden geprüft, überprüft und manchmal gehen sie auch verloren.
Bild: Kathryn Conrad & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

betroffen war, die die Unterlagen von einem Staat beschaffen musste, der sich in einer politisch instabilen Lage befand.

Der Fall veranschaulicht somit ein oft unterschätztes Risiko, nämlich die Folgen eines Verlusts von personenbezogenen Daten. Auch diesbezüglich müssen Schutzmaßnahmen ergriffen werden, z. B. im Falle von nicht zuordbaren Originaldokumenten ein Vier-Augen-Prinzip für deren Löschung, Nachforschungspflichten oder die Prüfung einer Kontaktaufnahmemöglichkeit zum Inhaber (vgl. Art. 5 Abs.1 Buchst. f) DS-GVO: Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor [...] unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung [...]).

Gerade weil die Verwaltung mit einer Vielzahl an sensibelsten Informationen von Bürger_innen zu tun hat, ist der sorgfältige Umgang mit ihnen so wichtig. Datenschutz ist kein Selbstzweck. Ziel ist immer der Schutz derjenigen Person, um deren Daten es geht, bzw. letztlich aller deren Rechte und Freiheiten. Diese können auch beim Verlust von Daten erheblich beeinträchtigt sein. Verantwortliche müssen deswegen auch diesbezügliche Risiken berücksichtigen und ihre Beschäftigten dafür sensibilisieren. Denn nur so können im Falle einer Datenpanne adäquate Maßnahmen getroffen werden, um mindestens mögliche (Folge-)Schäden abzumildern.

5.3.6. Auskunftspflicht bei Rechtsanwält_innen

Art. 57 Abs.1 Buchst. f) DS-GVO

Art. 15 DS-GVO gewährt jeder betroffenen Person ein Auskunftsrecht gegenüber der verantwortlichen Stelle zu den über sie gespeicherten personenbezogenen Daten. Auch wenn dieses Recht gegenüber Berufsgeheimnisträgern wie Rechtsanwält_innen eingeschränkt ist, ist von diesen immer zu prüfen, ob zumindest Teilauskünfte erteilt werden können.

Über die Polizei erreichte uns eine Beschwerde über eine Rechtsanwaltskanzlei. Diese hatte Forderungsschreiben an eine alte Adresse der beschwerdeführenden Person übermittelt. Die beschwerdeführende Person teilte der Kanzlei ihre neue Anschrift mit und beantragte kurze Zeit später eine Datenauskunft nach Art. 15 DS-GVO.

Die Kanzlei lehnte die Auskunftserteilung mit einem Verweis auf die Einschränkung des Auskunftsrechts nach § 29 Bundesdatenschutzgesetz (BDSG), die Verschwiegenheitspflicht nach §43a Bundesrechtsanwaltsordnung (BRAO) sowie Strafbarkeit der Verletzung von Privatgeheimnissen nach § 203 Strafgesetzbuch (StGB) ab. Nach der daraufhin eingehenden Beschwerde forderten wir die Kanzlei auf, das Auskunftsersuchen erneut zu prüfen und stellten zudem die Rechtsgrundlage hierfür dar.

Gemäß Art. 15 Abs.1 DS-GVO hat jede betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf weitere Informationen, die in Art. 15 Abs.1 Buchst. a) – h) gelistet werden.

Art. 23 Abs.1 DS-GVO erlaubt es den Mitgliedstaaten die Betroffenenrechte durch Rechtsvorschriften in einigen Bereichen zu beschränken, wenn bestimmte Voraussetzungen erfüllt sind. Deutschland hat von dieser Möglichkeit Gebrauch gemacht und in § 29 BDSG eine solche Rechtsvorschrift geschaffen.

Nach § 29 Abs.1 S.2 BDSG besteht das Recht auf Auskunft somit nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden Interessen eines Dritten geheim gehalten werden müssen. Bei der Verschwiegenheitspflicht der Rechtsanwält_innen, die sich aus § 43 a Abs. 2 BRAO ergibt, handelt es sich um eine solche Rechtsvorschrift.

Die Verschwiegenheitspflicht bezieht sich auf alles, was dem/der Rechtsanwält_in in Ausübung seines/ihres Berufes bekanntgeworden ist. Sie gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen (häufig z. B. bereits genutzte Adressdaten).

Es ist bei der Prüfung für jede Datenkategorie aus Art. 15 Abs.1 DS-GVO einzeln festzustellen, ob Auskunft gegenüber der betroffenen Person, die das Auskunftsersuchen gestellt hat, erteilt werden kann. In Betracht kommen daher auch Teilauskünfte.

Auch uns gegenüber teilte die Kanzlei mit, dass sie der Auffassung sei, dass aufgrund des § 29 Abs.1 S.2 BDSG kein Auskunftsrecht bestehe. Alle Informationen über die betroffene Person habe sie als Berufsgeheimnisträger erhalten, sodass das Auskunftsrecht ausgeschlossen sei.

Da auch auf unser erneutes Schreiben, in dem die Rechtslage nochmals dargestellt wurde, die Kanzlei bei ihrer Rechtsaufassung blieb, erließen wir eine Anweisung nach Art. 58 Abs.2 Buchst. c) DS-GVO, das Auskunftsersuchen erneut zu prüfen und entsprechend der durch uns dargestellten Rechtslage zu beauskunften.

Gegen diese Anweisung hat die Kanzlei nun Klage beim zuständigen Verwaltungsgericht Stuttgart eingelegt. Eine Entscheidung ist in dieser Sache noch nicht ergangen. Wir werden über den Ausgang des Verfahrens berichten.

5.3.7. Das haben wir schon immer so gemacht

Art. 57 Abs.1 Buchst. a), f) DS-GVO

Prozesse, welche sich über viele Jahre, häufig Jahrzehnte etabliert haben, müssen in regelmäßigen Abständen angeschaut und überprüft werden, u.a. ob diese noch den aktuellen (datenschutz-)rechtlichen Bestimmungen entsprechen oder ob eine Anpassung notwendig ist. Dies gilt auch für Löschkonzepte.

In diesem Jahr gingen bei uns mehrere Beschwerden im Zusammenhang mit der Speicherung und Löschung von Dokumenten in der Fahrerlaubnisakte ein. Hierbei wurde uns immer ein ähnlicher Sachverhalt geschildert. So berichteten die betroffenen Personen, dass sie in der Vergangenheit aufgrund von Zweifeln an ihrer Fahreignung ein medizinisch-psychologisches Gutachten beibringen mussten. In allen Fällen wurde sodann nach Einholung des Gutachtens die Fahrerlaubnis (wieder) erteilt. Jahre später nahmen die betroffenen Personen aus unterschiedlichen Gründen Einsicht in ihre Fahrerlaubnisakte und mussten dabei überrascht feststellen, dass darin weiterhin die Dokumente zur medizinisch-psychologischen Untersuchung und alle damit zusammenhängen Unterlagen vorhanden waren. Unter diesen Dokumenten auch Unterlagen von Ereignissen, welche schon über 10 Jahre zurücklagen und in keinem anderen Register mehr gespeichert waren. Es handelt sich überwiegend um Daten nach Art. 9 und 10 DS-GVO, also um besonders sensible Informationen über die betroffenen Personen.

Auf Nachfrage bei den verantwortlichen Stellen erhielten wir nicht immer nachvollziehbare Antworten. Insbesondere konnte uns keine verantwortliche Stelle nachvollziehbar erläutern, aus welchem Grund es nach einer erfolgreichen medizinisch-psychologischen Untersuchung und Erteilung der Fahrerlaubnis erforderlich sein sollte, diese Dokumente weiter aufzubewahren, da die Zweifel an der Fahreignung zumindest im Zusammenhang mit den damaligen Erkenntnissen durch das medizinisch-psychologische Gutachten ausgeräumt wurden. Die Frist für die Speicherung von Dokumenten in der Fahrerlaubnisakte richtet sich nach spezialgesetzlichen Regelungen aus dem Straßenverkehrsgesetz und nach den allgemeinen Grundsätzen.

Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse sind grundsätzlich nach spätestens zehn Jahren zu vernichten, es sei denn, mit ihnen im Zusammenhang stehende Eintragungen sind im Fahreignungsregister oder im Zentralen Fahrerlaubnisregister nach den Bestimmungen für diese Register zu einem früheren oder späteren Zeitpunkt zu tilgen oder zu löschen, in diesem Fall ist für die Vernichtung oder Löschung der frühere oder spätere Zeitpunkt maßgeblich, § 2 Abs.9 Straßenverkehrsgesetz (StVG). Für diese Unterlagen hat der Gesetzgeber mithin eine Höchstspeicherfrist festgelegt bzw. den Gleichlauf mit dem Fahreignungsregister und Zentralen Fahrerlaubnisregister.

Eine weitere spezielle Regelung findet sich in § 2 Abs.12 StVG. Soweit die mitgeteilten Informationen der Polizei über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, für die Beurteilung der Eignung oder Befähigung nicht erforderlich sind, sind die Unterlagen unverzüglich zu vernichten. Hierdurch ist es der Fahrerlaubnisbehörde nur in einem „engen zeitlichen Rahmen“ gestattet, Erkenntnisse über die fahreignungsrelevanten Eigenschaften eines Fahrerlaubnisinhabers zunächst zu sammeln (vgl. VGH Mannheim vom 28. Oktober 2004, Az. 10 S 475/04).

Hat der Gesetzgeber keine explizite Speicherfrist festgelegt, so richtet sich die Speicherung nach den allgemeinen Grundsätzen, insbesondere nach dem Grundsatz

der Speicherbegrenzung, Art. 5 Abs.1 Buchst. e DS-GVO. Danach müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für den Zweck, für die sie verarbeitet werden, erforderlich ist. So ergeben sich bspw. die Voraussetzungen für den Antrag auf Erteilung der Fahrerlaubnis aus § 21 Fahrerlaubnisverordnung (FeV). Danach sind dem Antrag verschiedene Unterlagen beizulegen, insbesondere diejenigen nach § 21 Abs. 3 Nr. 1 – 6 FeV, u.a. ein Lichtbild (§ 21 Abs. 3 Nr. 2 FeV), ein Nachweis über die Schulung in Erster Hilfe (§ 21 Abs. 3 Nr. 2 FeV) etc. Für diese Unterlagen, welche für die Beantragung der Fahrerlaubnis erforderlich sind, hat der Gesetzgeber keine explizite Speicherfrist festgelegt. Die Unterlagen, welche nach § 21 FeV für den Antrag auf Erteilung einer Fahrerlaubnis vorzulegen sind, werden zum Nachweis, dass die Voraussetzungen für die Erteilung der Fahrerlaubnis erfüllt waren, gespeichert. Die Speicherung dieser Daten ist mithin so lange die Fahrerlaubnis besteht, erforderlich. Bei anderen Unterlagen, welche nicht von § 2 Abs. 9 StVG oder § 2 Abs. 12 StVG erfasst sind, muss sich mithin im Einzelfall die Frage gestellt werden, ob diese für den Zweck, für welche sie erhoben worden sind, noch erforderlich sind. Ist dies nicht der Fall, sind diese zu löschen.

Die Fahrerlaubnisbehörden des Landes sollten ihr Löschkonzept im Zusammenhang mit der Speicherung und Löschung von Dokumenten in der Fahrerlaubnisakte nach den oben ausgeführten Kriterien durchsehen, ggf. anpassen und Maßnahme ergreifen, sofern Dokumente in Akten entgegen den obigen Ausführungen gespeichert sein sollten. Sofern kein Löschkonzept vorhanden sein sollte, so ist dringend eines zu erstellen und die vorhandenen Fahrerlaubnisakten ggf. entsprechend zu bereinigen.

5.3.8. Hilfe, die Daten meiner Kinder sind im Netz!

Art. 57 Abs.1 Buchst. a), f) DS-GVO

Die Rechtsgrundlage der Einwilligung (Art. 6 Abs.1 Buchst. a) DS-GVO) ist für öffentliche Stellen nicht ausgeschlossen. Allerdings müssen auch öffentliche Stellen, sofern sie die Verarbeitung von personenbezogenen Daten auf diese Rechtsgrundlage stützen möchten, einiges beachten, um die Voraussetzungen einer wirksamen Einwilligung zu erfüllen.

Immer wieder erreichen uns Beschwerden, in welchen uns betroffenen Personen darüber berichten, dass ihre Daten oder diejenigen ihrer Kinder ohne Rechtsgrundlage veröffentlicht wurden. Auf Nachfrage bei der verantwortlichen Stelle erhalten wir dann in manchen Fällen die Antwort, dass die Rechtsgrundlage eine Einwilligung sei. Bei näherem Hinsehen müssen wir dann immer wieder feststellen, dass die Voraussetzungen einer wirksamen Einwilligung nicht erfüllt waren.

So erreichte uns in diesem Jahr bspw. die Beschwerde eines Elternteils, welches darüber berichtete, dass der Name, Vorname und weitere Daten seines Kindes im Rahmen eines Stadtlaufes auf der Website der öffentlichen Stelle ohne die Zustimmung des Elternteils veröffentlicht wurden. In einem anderen Fall wurde sich darüber beschwert, dass im Zusammenhang mit der Durchführung des Sommerferienprogrammes durch eine öffentliche Stelle öffentlich Listen der teilnehmenden Kinder mit Namen, Vorname und Anschrift ausgehängt wurden.

Beide verantwortliche Stellen gaben als Rechtsgrundlage für die Veröffentlichung die Einwilligung nach Art. 6 Abs.1 Buchst. a) DS-GVO an. Bei Durchsicht der übersandten Unterlagen mussten wir allerdings in beiden Fällen feststellen, dass die Voraussetzungen einer wirksamen Einwilligung nicht erfüllt waren, obwohl die Verarbeitungen grundsätzlich aufgrund einer Einwilligung hätte erfolgen können. U.a. wäre es in beiden Fällen nicht möglich gewesen, das Kind zum Stadtlauf bzw. Ferienprogramm anzumelden, ohne auch die „Zustimmung“ zur Veröffentlichung auf der Website bzw. dem öffentlichen Aushang zu geben, sodass es schon an der Freiwilligkeit fehlte.

Die Bedingungen für die Einwilligung finden sich in Art. 7 DS-GVO, u.a. muss die verantwortliche Stelle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat, Art. 7 Abs.1 DS-GVO. Eine wirksame Einwilligung muss freiwillig, bestimmt, informiert und unmissverständlich sein, Art. 4 Nr. 11 DS-GVO. Entscheidend sind dabei immer die konkreten Umstände des Einzelfalls. Eine Einwilligung ist dann freiwillig, wenn die betroffene Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“ (Erwägungsgrund (EG) 42 zur DS-GVO). Arbeiten öffentliche Stellen mit Einwilligungen als Rechtsgrundlage für ihre Datenverarbeitung, ist das Merkmal der

Freiwilligkeit besonders sorgfältig zu prüfen. Denn im Verhältnis öffentliche Stelle – Bürger_in liegt ein strukturelles Ungleichgewicht, welches die Freiwilligkeit einer Willensbekundung des Bürgers grundsätzlich in Frage stellt (EG 43 zur DS-GVO). Die Einwilligung gilt dann nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht wäre (EG 43 zur DS-GVO). Daneben muss der Zweck der Datenverarbeitung bestimmt sein (Bestimmtheit). Die betroffene Person muss u.a. wissen, wer die verantwortliche Stelle ist und für welche Zwecke ihre Daten verarbeitet werden (Informiertheit). Schließlich muss die Einwilligung „unmissverständlich" erfolgen, also durch eine eindeutige bestätigende Handlung. Dabei können Stillschweigen oder Untätigkeit keine Einwilligung darstellen (EG 32 zur DS-GVO).

Auch sollten öffentliche Stellen berücksichtigen, sofern sie ihrer Datenverarbeitung auf eine Einwilligung stützen wollen, dass die Einwilligung jederzeit ohne Angabe von Gründen widerrufen werden kann. Hierauf ist die betroffene Person vor der Abgabe hinzuweisen. Die Rechtsmäßigkeit der Verarbeitung bis zum Widerruf, sofern eine wirksame Einwilligung vorlag, ist hiervon nicht berührt, Art. 7 Abs. 3 DS-GVO.

In den geschilderten Fällen wäre es grundsätzlich möglich gewesen, die Verarbeitung auf eine Einwilligung zu stützen, allerdings müssten hierfür die Prozesse entsprechend angepasst werden. Im Zusammenhang mit der Veröffentlichung von Daten von Minderjährigen sollte immer beachtet werden, dass es sich um eine besonderes vulnerable Personengruppe handelt, welche besonders zu schützen ist. Sodass zu empfehlen ist – sofern überhaupt notwendig – möglichst wenig Daten über das einzelne Kind zu veröffentlichen.

In bestimmten Konstellationen ist es auch für öffentliche Stellen möglich, die Verarbeitung von personenbezogenen Daten auf eine Einwilligung nach Art. 6 Abs.1 Buchst. a) DS-GVO zu stützen. Sollte dies in Betracht gezogen werden, so sind die Voraussetzungen einer Einwilligung besonders sogfältig zu prüfen, insbesondere die Freiwilligkeit. Ein Schriftformerfordernis für die Einwilligung sieht die DS-GVO zwar nicht vor, im Hinblick auf die Nachweispflicht der verantwortlichen Stelle ist sie aber zu empfehlen.

Infokasten

Weitere Informationen zur Einwilligung stehen in der Broschüre „Datenschutz bei Gemeinden", ab S.16: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Brosch%C3%BCre-Gemeinden-November-2019.pdf

Bild: Annett Seidler-stock.adobe.com

5.4. Abteilung 3: Gesundheits-, Sozial-, Bildungs- und Justizwesen

In dieser Abteilung befassen wir uns unter anderem mit dem gesamten Gesundheitsbereich, von der Arztpraxis über Krankenhäuser bis hin zum Pflegedienst. Auch sitzen hier unsere Fachleute aus dem Bildungsbereich und dem Justizwesen.

5.4.1. Datenpannen im Gesundheitswesen

Art. 57 Abs.1 Buchst. a), d), h)

In der täglichen Arbeit kümmerte sich unser Team um zahlreiche Meldungen von sogenannten „Datenpannen“ durch die unserer Aufsicht unterliegenden datenschutzrechtlich Verantwortlichen. Die nachfolgenden Problemaufrisse rund um das Thema „Versand“ von personenbezogenen Daten im Gesundheitswesen sollen beispielhaft die aufsichtsbehördliche Praxis bei der Bearbeitung von Meldungen nach Art. 33 DS-GVO näher beleuchten sowie die Verantwortlichen im Zusammenhang mit der Verarbeitung personenbezogener Daten sensibilisieren.

Patientendaten auf mobilen Datenträger bitte nur verschlüsselt und gut verpackt verschicken

Werden insbesondere digitale Patientendaten und damit Gesundheitsdaten als besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs.1 DS-GVO, auf einem mobilen Datenträger postalisch versandt, so müssen die darauf befindlichen Daten angemessen und nach Stand der Technik verschlüsselt werden (vgl. Art. 24, Art. 32 Abs.1 DS-GVO).

Werden dagegen etwa Arztbriefe oder vollständige Patientenakten in Papierform postalisch übermittelt, entsteht schnell eine große Menge an sensiblen Dokumenten. Wenn der Datenempfänger diese Datenmenge elektronisch weiterverarbeiten will, so steht ihm ein Scanvorgang der Papierunterlagen als aufwendiger Zwischenschritt bevor. Nicht selten wird zur Vereinfachung in der Praxis daher auf den Versand einer sogenannten digitalen Datenkopie auf einem mobilen Datenträger (z. B. USB-Stick oder CD) zurückgegriffen, wenn keine Webportallösung mit sicher verschlüsselter Übertragung, Verschlüsselung auch gegenüber dem Portalanbieter und hinreichend sicheren Authentifizierungsmöglichkeiten zur Verfügung steht.

Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO im Zusammenhang mit verloren gegangenen Trägermedien beim Postversand sind keine Seltenheit in unserer aufsichtsrechtlichen Behördenpraxis. So sei nur beispielhaft genannt, dass beim Postversand wiederholt Fehlversendungen zu verzeichnen sind und Sendungen die Adressaten teilweise überhaupt nicht erreichen. Zudem können Versandumschläge beim Versandprozess beschädigt werden und kleine Trägermedien herausfallen. Sich optisch abzeichnende Gegenstände in Briefumschlägen lassen sich im Übrigen leicht ertasten und können – unter Aufbringen einer gewissen kriminellen Energie – zur Herausnahme des Mediums verleiten.

Was ist also zu tun? Anders als Papiersendungen lassen sich Trägermedien angemessen nach dem aktuellen Stand der Technik verschlüsseln (dafür geeignete Verfahren empfiehlt das BSI in seiner Technischen Richtlinie BSI TR-02102). Auf diese Weise sind beim Verlust der Postsendung oder des Datenträgers die personenbezogenen Daten nicht lesbar, sollten die sensiblen Inhalte buchstäblich „in falsche Hände“ geraten. Zudem empfehlen wir den Verantwortlichen, gepolsterte Umschläge mit verstärkten Seiten zu nutzen. Das Festkleben des Datenträgers am Anschreiben verhindert zusätzlich unnötige Bewegungen der CD / des USB-Sticks selbst.

Darüber hinaus empfehlen wir, bei sensiblen Sendungen eine Sendungsnachverfolgung einzurichten, damit bei einem Verlust möglichst Feststellungen zum Verbleib der Sendung getroffen werden können. Denn auch bei verschlüsselter Versendung ist zu bedenken, dass möglicherweise später infolge der Veralterung von Verschlüsselungsverfahren (bzw. infolge zunehmender Entschlüsselungsmöglichkeiten) der Inhalt der Sendung zur Kenntnis genommen werden kann. Bei umfangreichen Datentransfers mit sensiblen Daten halten wir die Verwendung von solchen Trackingmaßnahmen für geboten (vgl. unseren 38. Tätigkeitsbericht Datenschutz 2022, S. 91).

Kommt öfter vor: Unterlagen landen beim falschen Empfänger

Wiederum häuften sich im Berichtszeitraum die Meldungen von Verletzungen des Schutzes personenbezogener Daten wegen des Versands von Unterlagen an unberechtigte Empfänger. So bildete der Fehlversand ganzer Schreiben und / oder von deren Anlagen einen Schwerpunkt der eingegangenen Datenpannenmeldungen nach Art. 33 DS-GVO im Jahr 2025.

In zahlreichen Fällen gingen somit Gesundheitsdaten im Sinne von Art. 4 Ziff. 15 DS-GVO von Patienten z. B. ärztliche Befunde postalisch an falsche Adressaten, wodurch Dritte oftmals ungewollt Kenntnis erhielten.

Als Grund für den Fehlversand wurde dabei häufig unter anderem eine Fehladressierung, die Verwechslungen aufgrund von Namensgleichheit, eine fehlerhafte Zusammenstellung von Unterlagen im organisatorischen Tagesbetrieb oder eine hiermit einhergehende falsche Kuvertierung angegeben. Sehr häufig identifizierten die Verantwortlichen aber schlicht „menschliches Versagen“ als Ursache für den Fehlversand. Deswegen erachteten sie oftmals als Maßnahme zur Vermeidung von Wiederholungen vergleichbarerer Datenpannen ausschließlich eine Sensibilisierung von Einzelpersonen als ausreichend.

Die konkrete Ausganslage hinsichtlich der technischen und organisatorischen Maßnahmen wurde dagegen leider nur selten analysiert. In der Folge wurden konkrete Vorfeldmaßnahmen zur Verhinderung des Fehlversands kaum in dem gebotenen Maß erwogen und als technisch-organisatorische Maßnahme verbessernd in den Tagesbetrieb implementiert.

Nach Art. 24 Abs. 1 DS-GVO setzt der Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung im Einklang mit der DS-GVO erfolgt.

In Konkretisierung des Grundsatzes der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f) DS-GVO) verlangt Art. 32 Abs. 1 DS-GVO von dem Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen sind in erforderlichem Umfang zu überprüfen und zu aktualisieren (vgl. Art. 24 Abs. 1 Satz 2 DS-GVO).

Versehentliche Fehlversendungen lassen sich zwar auch bei Vorhandensein von angemessenen technisch-organisatorischen Maßnahmen nicht vollständig ausschließen. Unerlässlich ist dennoch, dass die nötigen technisch-organisatorischen Maßnahmen überhaupt ergriffen, regelmäßig auf ihre Bewährtheit evaluiert und bei Bedarf zielgerichtet angepasst werden. Und insbesondere bei einer Datenpanne hat der Verantwortliche die Notwendigkeit von Abhilfemaßnahmen zu überprüfen und der Aufsichtsbehörde im Rahmen einer Meldung so zu schildern, dass eine Überprüfung der Angemessenheit ermöglicht wird (vgl. insbesondere Art. 33 Abs. 3 Buchst. d) und ferner Abs. 5 DS-GVO).

Welche Frau Müller noch mal?

Insbesondere eine Namensgleichheit dürfte bei der mitunter hohen Anzahl beispielsweise der von Kliniken oder der Ärzteschaft verarbeiteten personenbezogenen Daten vermehrt vorkommen, sodass diesbezüglich möglichst zuverlässige Maßnahmen getroffen werden müssen. Namen allein sind nicht ausreichend für eine eindeutige Patientenzuordnung. Wir empfehlen stattdessen, eine Kombination von Identifikationsmerkmalen zu nutzen, wie etwa die eines Geburtsdatums oder einer Patienten-ID. In technischer Hinsicht lassen sich zudem Validierungsregeln implementieren, die beispielsweise Warnhinweise bei Namensidentität aufzeigen.

Die Schaffung von klaren organisatorischen Prozessen bewirkt zudem Sicherheit für Beschäftigte und vermeidet Fehler im oftmals stressigen und schnelllebigen Tagesgeschäft. Folgende Prozesse lassen sich beispielhaft abbilden:

- Erstellung von Arbeits- bzw. Dienstanweisungen für den Postversand, verschlüsselten E-Mail-Versand sowie die Aktenzuordnung
- Checklisten-Prüfung vor dem Versand
- klare und dokumentierte Zuständigkeiten
- Ausgestaltung des Druckvorgangs dahingehend, dass Fehlsortierungen möglichst ausgeschlossen werden
- regelmäßige Datenschutzschutzschulungen unter Beleuchtung der konkret aufgetretenen Fehlerquellen

- Überprüfung von Postausgängen im sog. „Vier-Augen-Prinzip“, insbesondere bei sensiblen und quantitativ umfangreichen Versandvorgängen

Fehlversand – was tun?

Eine Datenpanne hat der Verantwortliche nicht nur zum Anlass zu nehmen, seine technischen und organisatorischen Maßnahmen zu überprüfen, er muss gegebenenfalls auch Maßnahmen ergreifen, um mögliche nachteilige Auswirkungen der Datenpanne für die konkret von ihr betroffenen Personen abzumildern. Für den Fall, dass es trotz aller ergriffenen technisch-organisatorischen Maßnahmen zu einem Fehlversand kommt, sollte deswegen auch ein besonderes Augenmerk auf die Auswahl der zu ergreifenden Abmilderungsmaßnahmen gelegt werden.

Hierzu gehört, dass der Empfänger des Irrläufers zur Rücksendung aufgefordert wird. Dabei sollte die Rückführung der Sendung für den Fehladressaten möglichst einfach ausgestaltet werden, z. B. durch Überlassung eines ausreichend frankierten Freiumschlags oder durch Abholung des Fehlversandes. Eine Rücksendung ermöglicht dem Verantwortlichen die datenschutzgerechte weitere Aufbewahrung oder Vernichtung der Daten. Anders als bei einer bloßen Aufforderung, die Unterlagen zu vernichten, lässt sich durch eine Rücksendung verhindern, dass das Schreiben beim Empfänger etwa im Hausmüll entsorgt wird, was wiederum ein nicht geringes Missbrauchsrisiko durch weitere Personen zur Folge haben würde.

Wir empfehlen zudem gegenüber dem Fehlempfänger ein Verwertungsverbot in Bezug auf die personenbezogenen Daten Dritter auszusprechen. Der Fehlempfänger sollte zusätzlich aufgefordert werden, Verschwiegenheit über die ihm unrechtmäßig bekannt gewordenen Daten zu bewahren. Außerdem sollte er gebeten werden zu versichern, dass er die Daten vollständig zurückgegeben, also insbesondere keine Kopien gefertigt und zurückbehalten hat.

„Menschliches Einzelversagen“ spielt im Ergebnis dann eine untergeordnete Rolle, wenn der Verantwortliche mögliche Fehlerquellen vorab identifiziert hat und diesen vorausschauend begegnet ist.

Wie man der statischen Erfassung zu eingegangenen Datenpannenmeldungen im Berichtszeitraum entnehmen kann, steigt die Zahl stetig an. Für den Umgang mit Datenpannen insbesondere in den Bereichen Wirtschaft und Gesundheitswesen sehen wir ein hohes Schulungsbedürfnis der Verantwortlichen. Unsere Schulung „Grundlagen des Datenpannen-Managements“ in unserem hauseigenen Bildungszentrum für Datenschutz und Informationsfreiheit – BIDIB erfreute sich auch im Jahr 2025 einer sehr großen Beliebtheit.

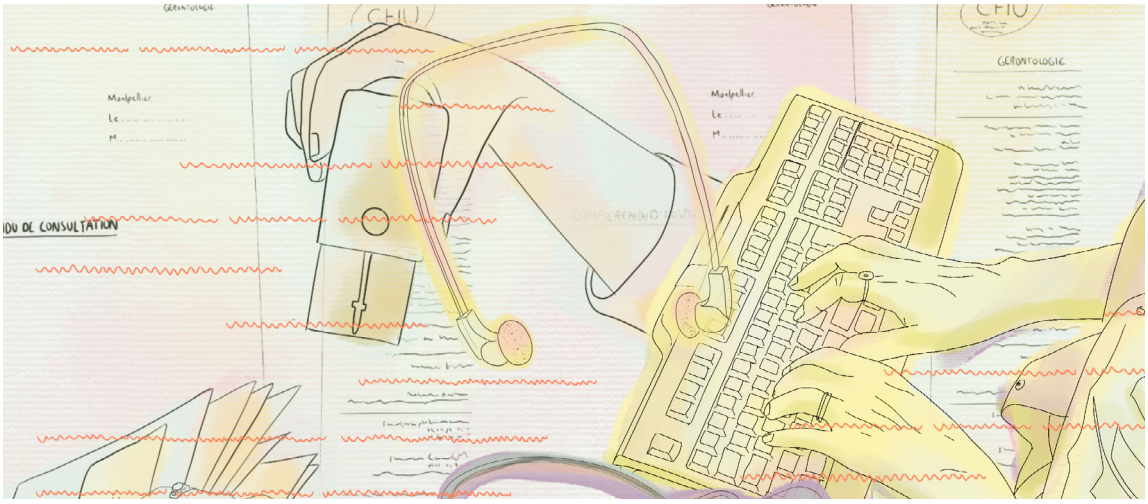


Bild: Fanny Maurel & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

5.4.2. Das Recht auf Auskunft in der Kinder- und Jugendhilfe

Art. 57 Abs.1 Buchst. a), d), f) DS-GVO

Auch in diesem Berichtszeitraum hat uns das Auskunftsrecht wieder in vielen Bereichen beschäftigt. Dies gilt auch für den Bereich der Kinder- und Jugendhilfe. Dort herrschte insbesondere auf Seiten der Jugendämter oft Unsicherheit hinsichtlich der Frage, inwieweit gemäß Art. 15 DS-GVO Auskunft erteilt werden kann und muss. Im Folgenden soll daher ein kurzer, nicht abschließender Überblick über die Besonderheiten bei der Auskunftserteilung im Bereich der Kinder- und Jugendhilfe in öffentlicher Trägerschaft gegeben werden. Dabei ist zu betonen, dass sich die Frage, inwieweit einem konkreten Auskunftsersuchen nachzukommen ist, stets einzelfallbezogen zu beantworten ist. Auch wenn wir natürlich die Übersicht möglichst einfach halten wollen, kommen wir hier nicht umhin, juristisch etwas ausführlicher zu werden.

Im Berichtszeitraum waren wir auch im Bereich der Kinder- und Jugendhilfe wieder mit Beschwerden befasst, die eine nicht vollständige oder unterbliebene Erfüllung von Auskunftsersuchen gemäß Art. 15 DS-GVO betrafen. Oft sind es Eltern(-teile), die ein Interesse daran haben, zu erfahren, welche personenbezogenen Daten über sie selbst oder ihre Kinder verarbeitet werden, und deswegen ein Auskunftsersuchen geltend machen.

I. Antragstellende Person

Im Bereich der Kinder- und Jugendhilfe machen die antragstellenden Personen das Auskunftsrecht gemäß

Art. 15 DS-GVO oftmals nicht nur in Bezug auf die eigenen, sondern z. B. auch im Hinblick auf personenbezogene Daten des anderen Elternteils oder der Kinder geltend. Hier ist von den verantwortlichen Stellen besondere Sorgfalt auf die Prüfung zu legen, ob eine entsprechende Vertretungsbefugnis vorliegt.

Wird eine solche nicht nachgewiesen, kann die antragstellende Person das Auskunftsrecht nur bezüglich der eigenen Daten geltend machen. Mithin ist bei der Erteilung der Auskunft darauf zu achten, dass diese nur mit Blick auf die antragstellende Person beziehungsweise von ihr wirksam vertretene Personen erteilt wird.

II. Auskunftsrecht gemäß Art. 15 DS-GVO und Akteneinsichtsrecht gemäß § 25 SGB X

Zu beachten ist auch, dass sich das Akteneinsichtsrecht nach § 25 Sozialgesetzbuch Zehntes Buch (SGB X) und das Auskunftsrecht nach Art. 15 DS-GVO zwar vielfach überschneiden, es sich hierbei jedoch um unterschiedliche Ansprüche handelt, die sowohl hinsichtlich der Voraussetzungen als auch des Umfangs der Beantwortung auseinanderfallen können. Eine allgemeine Übersicht zu Informationszugangsrechten bei öffentlichen Stellen findet sich unter: https://www.baden-wuerttemberg.datenschutz.de/zugangsrechte-neben-lifg/.

III. Mögliche Einschränkungen

Im Sozialdatenschutz gibt es zum Auskunftsrecht besondere Vorschriften (s. auch 36. Tätigkeitsbericht, S. 94 ff.). Diese sehen auch Einschränkungen vor. Daneben finden sich in Art. 15 Abs. 4 DS-GVO und Art. 12 Abs. 5 Satz 2 Buchst. b) DS-GVO allgemeine Einschränkungen des Auskunftsrechts. Allen Einschränkungen des Auskunftsrechts ist gemein, dass grundsätzlich eine enge Auslegung geboten ist. Dies gilt insbesondere mit Blick auf pauschale Einschränkungen. Vor allem hat der Verantwortliche zu berücksichtigen, dass anstelle einer Nichterteilung der Auskunft Schwärzungen als milderes Mittel anzusehen sind, sofern dadurch entgegenstehende (Dritt-)Interessen gewahrt werden. Die Auskunft über personenbezogene Daten, für die keine Einschränkungen einschlägig sind, darf nicht deswegen verweigert werden, weil für andere Daten eine solche Beschränkung besteht. Vom Auskunftsrecht umfasst sind dabei im Allgemeinen auch solche Daten, die der antragstellenden betroffenen Person bereits bekannt sind (siehe auch BGH, Urteil vom 15.06.2021 – VI ZR 576/19, NJW 2021, 2726).

1. § 83 SGB X

Besondere sozialrechtliche Einschränkungen finden sich im Sozialdatenschutz zunächst in § 83 SGB X (s. auch unseren 36. Tätigkeitsbericht Datenschutz 2020, S. 94 ff.). Im Folgenden werden einzelne Aspekte dieser Vorschrift herausgegriffen.

a) § 83 Abs. 1 SGB X

Die Regelung in § 83 Abs. 1 SGB X enthält zwei Fallgruppen (Nummer 1 und 2), in denen Ausnahmen von der Auskunftspflicht geregelt werden.

aa) § 83 Abs. 1 Nummer 1 SGB X

Nach § 83 Abs. 1 Nummer 1 SGB X besteht das Recht auf Auskunft dann nicht, wenn die betroffene Person nach § 82a Abs. 1, 4 und 5 SGB X nicht (gemäß Art. 14 DS-GVO) zu informieren ist.

Insoweit wird also auf drei Absätze des § 82a SGB X Bezug genommen:

(1) Nach § 82a Abs. 1 SGB X besteht die Informationspflicht aus Art. 14 DS-GVO in drei Fällen nicht, nämlich

1. soweit die Erteilung der Information die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verant-

Infokasten

Der Überblick versteht sich als Ergänzung zu den bereits in unserem 36. Tätigkeitsbericht für das Jahr 2020 zur Auskunft im Sozialdatenschutz enthaltenen Ausführungen: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf , S. 94 ff. Diese Ausführungen sollen nun im vorliegenden 41. Tätigkeitsbericht mit Blick auf die Kinder- und Jugendhilfe ergänzt werden. Dabei ist zu betonen, dass die Frage, inwieweit einem konkreten Auskunftsersuchen nachzukommen ist, stets einzelfallbezogen zu beantworten ist. Die Ausführungen beziehen sich ausdrücklich nur auf die Kinder- und Jugendhilfe in öffentlicher Trägerschaft.

wortlichen liegenden Aufgaben gefährden würde (§ 82a Abs.1 Nummer 1 Buchst. a) SGB X),

2. soweit die Erteilung der Information die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde (§ 82a Abs.1 Nummer 1 Buchst. a) SGB X) und

3. soweit die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten geheim gehalten werden müssen (§ 82a Abs.1 Nummer 2 SGB X, siehe auch Art. 15 Abs.4 DS-GVO).

Dies gilt in allen genannten Fällen nur, sofern aus den jeweils genannten Gründen das Interesse der betroffenen Person zurücktreten muss (§ 82a Abs.1 2. Halbsatz SGB X). Entsprechend ist stets eine Interessenabwägung durchzuführen, bei der grundsätzlich strenge Maßstäbe anzulegen sind (s.aber noch unten zu § 65 SGB VIII).

(2) Die in § 83 Abs.1 Nummer 1 SGB X weiter in Bezug genommene Regelung in § 82a Abs.4 SGB X schränkt die Informationspflichten hinsichtlich der Empfängerkategorien der Daten ein und erklärt insoweit die Vorschriften aus § 82 Abs.1 SGB X für entsprechend anwendbar. Danach ist nur in den in § 82 Abs.1 SGB X aufgeführten Fällen eine Information über Empfängerkategorien vorzunehmen. Über die Empfängerkategorien ist mithin nur Auskunft zu erteilen, soweit

1. die betroffene Person nach den Umständen des Einzelfalles nicht mit der Nutzung oder der Übermittlung von Sozialdaten an diese Kategorien von Empfängern rechnen muss,

2. es sich nicht um Speicherung, Veränderung, Nutzung, Übermittlung, Einschränkung der Verarbeitung oder Löschung von Sozialdaten innerhalb eines Leistungsträgers oder einer anderen in § 35 des Ersten Buches genannten Stelle bzw. innerhalb der Organisationseinheit einer Gebietskörperschaft, die als Leistungsträger fungiert (s.§ 67 Abs.4 Satz 2 SGB X), handelt oder

3. es sich nicht um eine Kategorie von Leistungsträgern (oder anderen in § 35 des Ersten Buches genannten Stellen) oder von Organisationseinheiten innerhalb einer Gebietskörperschaft, die als Leistungsträger fungiert (vgl. § 67 Abs.4 Satz 2 SGB X), handelt, die auf Grund eines Gesetzes zur engen Zusammenarbeit verpflichtet sind.

Unabhängig hiervon bleibt aber die Auskunft über konkrete Empfänger zu erteilen, soweit solche bekannt sind (vgl. BeckOGK/Leopold, 15.11.2024, SGB X § 82 Rn. 23, § 82a Rn. 30).

(3) Die von § 83 Abs.1 Nummer 1 SGB X zuletzt in Bezug genommene Norm des § 82a Abs.5 SGB X sieht schließlich eine Einschränkung bei der Übermittlung von Sozialdaten durch öffentliche Stellen u.a. an Strafverfolgungs- und Sicherheitsbehörden vor und ist insoweit inhaltsgleich mit § 83 Abs.5 SGB X. Insoweit darf die Auskunft über die Übermittlung dieser Daten nur erfolgen, wenn die empfangende Stelle zugestimmt hat.

bb) § 83 Abs.1 Nummer 2 SGB X

Zudem wird durch § 83 Abs.1 Nummer 2 SGB X der Auskunftsanspruch dann ausgeschlossen, wenn die Sozialdaten nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn zusätzlich die Auskunftserteilung in diesen Fällen einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen als den genannten Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist. Die Vereinbarkeit dieser Norm mit der DS-GVO ist teilweise streitig (vgl. die Kritik an § 34 Abs.1 Nummer 2 BDSG z.B. Kühling/Buchner/Golla, 4. Aufl. 2024, BDSG § 34 Rn. 11 f.).

b) § 83 Abs.2 SGB X

Gemäß § 83 Abs.2 Satz 1 SGB X soll die betroffene Person in ihrem Auskunftsantrag die Art der Sozialdaten, über die Auskunft erteilt werden soll, näher bezeichnen. Hieran sind grundsätzlich keine zu hohen Anforderungen zu stellen. Vor Ablehnung eines Antrags ist vom Verantwortlichen auf eine Vervollständigung beziehungsweise Ergänzung durch die betroffene Person hinzuwirken.

Sind die Sozialdaten nicht automatisiert und (im Wortlaut des Gesetzes steht wohl zu Unrecht „oder“) nicht in Dateisystemen gespeichert, wird die Auskunft gemäß § 83 Abs.2 Satz 2 SGB X nur erteilt, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen und der für die Erteilung der

Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Diese Fälle liegen außerhalb des unmittelbaren sachlichen Anwendungsbereichs der DS-GVO, der eine (zumindest teilweise) automatisierte oder in einem Dateisystem erfolgende Datenverarbeitung voraussetzt (vgl. Art. 2 Abs.1 DS-GVO). Die Vorschriften der DS-GVO finden hier mithin von vornherein nur kraft einfach-gesetzlicher Erstreckung in § 35 Abs. 2 Satz 2 SGB I Anwendung. Die Auskunft wird in dieser Fallkonstellation auch bei ausreichenden Angaben zur Auffindung der Daten nur dann erteilt, wenn der für ihre Erteilung erforderliche Aufwand nicht unverhältnismäßig ist. Auch insoweit ist grundsätzlich ein strenger Maßstab für die Feststellung der Unverhältnismäßigkeit anzulegen.

Eine besondere Regelung über die Art und Weise der Auskunftserteilung enthalten sodann die Vorschriften des § 83 Abs. 2 Satz 3 und 4 SGB X. Insoweit ist insbesondere darauf hinzuweisen, dass nach § 83 Abs. 2 Satz 4 SGB X in Verbindung mit § 25 Abs. 2 SGB X die Behörde der betroffenen Person den Inhalt der personenbezogenen Daten durch einen Arzt vermitteln lassen kann, soweit diese Angaben über gesundheitliche Verhältnisse der betroffenen Person umfassen. Die Behörde soll dies tun, wenn zu befürchten ist, dass die Auskunft sonst der betroffenen Person einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde. Ähnliches gilt, soweit die zu beauskunftenden Daten Angaben enthalten, deren Bekanntgabe die Entwicklung und Entfaltung der Persönlichkeit der betroffenen Person beeinträchtigen können. In diesem Fall kann bzw. soll die Behörde die Auskunft durch eine Bedienstete oder einen Bediensteten der Behörde vermitteln, die bzw. der durch Vorbildung sowie Lebens- und Berufserfahrung dazu geeignet und befähigt ist. Zu beachten ist allerdings, dass diese Regelung aus dem SGB X die Vorgaben der DS-GVO nicht einschränken soll. Besteht die betroffene Person also auf einer Auskunft direkt ihr gegenüber, hat dies nach den Vorgaben der DS-GVO zu geschehen (Wiesner/Wapler/Walther, 6. Aufl. 2022, SGB X §§ 83, 25 Rn. 24; BeckOGK/Leopold, 15.11.2024, SGB X § 83 Rn. 51).

c) § 83 Abs. 3 SGB X

Zu beachten ist auch, dass gemäß § 83 Abs. 3 Satz 1 SGB X die Gründe für die Auskunftsverweigerung zu dokumentieren sind. Hierfür sieht § 83 Abs. 3 Satz 2 SGB X eine Ausnahme für den Fall vor, dass durch Mitteilung der tatsächlichen und rechtlichen Gründe für die Ablehnung der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die betroffene Person ist jedoch gemäß § 83 Abs. 3 Satz 3 SGB X in diesem Falle (zusätzlich zur allgemeinen Informationspflicht gemäß Art. 13 Abs. 2 Buchst. d, Art. 14 Abs. 2 Buchst. e DS-GVO) darüber zu unterrichten, dass sie sich an die zuständige Aufsichtsbehörde wenden kann.

2. § 65 SGB VIII

Von besonderer Bedeutung in der Kinder- und Jugendhilfe ist § 65 Sozialgesetzbuch Achtes Buch (SGB VIII). Gemäß § 65 Abs.1 Satz 1 SGB VIII dürfen Sozialdaten, die einem bestimmten Mitarbeiter eines Trägers der öffentlichen Jugendhilfe zum Zwecke persönlicher und erzieherischer Hilfe anvertraut wurden, nur bei Vorliegen einer der dort genannten Ausnahmen weitergegeben oder übermittelt werden. Als anvertraut sind Daten dann anzusehen, wenn sie einer konkreten Fachkraft in der Jugendhilfe im Vertrauen auf ihre besondere Schutzpflicht in der Erwartung mitgeteilt worden sind, dass sie Dritten nicht zugänglich gemacht werden.

Für die jeweils infrage stehenden personenbezogenen Daten ist im Einzelfall durch die verantwortliche Stelle zu beurteilen, ob es sich jeweils um anvertraute Daten im Sinne von § 65 Abs.1 SGB VIII handelt. Über anvertraute Daten darf grundsätzlich nur der anvertrauenden Person eine auf diese beziehbare Auskunft nach Art. 15 DS-GVO erteilt werden. Mit § 65 SGB VIII soll nämlich nach der Rechtsprechung (vgl. z. B. VGH Baden-Württemberg, Beschluss vom 27.4.2020 – 12 S 579/20) das für eine persönliche und erzieherische Hilfe in der Kinder- und Jugendhilfe erforderliche besondere Vertrauensverhältnis zwischen der Fachkraft des Jugendamts und der Klientin/dem Klienten geschützt werden.

3. § 68 Abs. 3 SGB VIII

Im Bereich der Beistandschaft, Amtspflegschaft und Amtsvormundschaft ist eine Einschränkung des Auskunftsrechts in § 68 Abs. 3 SGB VIII verankert. Demnach besteht das Recht auf Auskunft nach § 68 Abs. 3 Satz 1 Alternative 1 i. V. m. § 68 Abs. 2 Satz 3 SGB VIII nur, soweit die Auskunft mit der Wahrung der Interessen der minderjährigen Person vereinbar ist und nicht die Erfüllung der Aufgaben gefährdet, die in der Zuständigkeit des Beistands, des Amtspflegers oder des Amtsvormunds liegen. Des Weiteren besteht gemäß § 68 Abs. 3 Satz 1 Alternative 2 SGB VIII das Recht auf Auskunft nicht, wenn durch die Auskunftserteilung berechtigte Interessen Dritter beeinträchtigt würden.

III. Rechtsbehelfe und weitere Möglichkeiten bei Ablehnung der Auskunftserteilung

Wird einer betroffenen Person durch einen Sozialleistungsträger oder eine andere Stelle nach § 35 SGB I keine Auskunft erteilt, kann sie sich gemäß § 83 Abs. 4 SGB X an die für die jeweilige Stelle zuständige Datenschutzaufsichtsbehörde wenden, um prüfen zu lassen, ob die Ablehnung rechtmäßig war. Alternativ kann sie bei dieser auch Beschwerde gemäß Art. 77 Abs. 1 DS-GVO in Verbindung mit § 81 Abs. 1 SGB X einlegen, wenn sie der Auffassung ist, dass die Ablehnung rechtswidrig war. Unbeschadet hiervon bleibt die Möglichkeit, ggf. Widerspruch einzulegen oder Klage vor dem zuständigen Gericht zu erheben. In aller Regel empfehlen wir aber, jedenfalls soweit nicht die Verfristung eines Widerspruchs oder einer Klageerhebung droht, sich zunächst an die oder den behördlichen Datenschutzbeauftragten zu wenden, die oder der die Entscheidung des Verantwortlichen auf kurzem Wege prüfen und ggf. erläutern oder sogar auf eine einvernehmliche Lösung hinwirken kann.

5.4.3. Keine pauschale Identitätskontrolle mittels eines Ausweisdokuments

Art. 57 Abs. 1 Buchst. f) DS-GVO

Eine Person teilte uns im Rahmen einer Beschwerde mit, dass sie die Übersendung ihrer eigenen personenbezogenen Daten, darunter auch Daten besonderer Kategorien, von einem datenschutzrechtlich verantwortlichen Krankenhaus begehrte. Das Krankenhaus kam diesem Wunsch nach und übersandte die Unterlagen postalisch an die anfragende Person. Diese wiederum sah sich aufgrund der unmittelbaren Übersendung der Akteninhalte in ihrem Persönlichkeitsrecht verletzt, weil die Unterlagen ohne die Durchführung einer Identitätskontrolle, insbesondere ohne die vorhergehende Anforderung ihres Ausweisdokuments, übermittelt wurden.

Im Ergebnis war nicht von einer Datenschutzverletzung auszugehen. Bezogen auf die Betroffenenrechte nach der Datenschutz-Grundverordnung (DS-GVO) werden in Art. 12 DS-GVO die Modalitäten für die Ausübung der Rechte der betroffenen Personen näher ausgeführt. Im Hinblick auf die Identifizierung der betroffenen Person, die von ihren Betroffenenrechten Gebrauch machen möchte, regelt Art. 12 Abs. 6 DS-GVO, dass die Verantwortliche bei objektiv begründeten Zweifeln an der Identität der Person zusätzliche Informationen zur Bestätigung der Identität verlangen kann.

Denkbar ist, dass in begründeten Einzelfällen – und damit nicht pauschal – zur Legitimation der Betroffenen die Vorlage eines Ausweisdokuments verlangt wird, um eine eindeutige Zuordnung der gespeicherten Daten zur Person vorzunehmen; bestehen in solchen Einzelfällen gute Gründe für die Vorlage eines Ausweisdokuments, werden allerdings regelmäßig nur der (Vor-)Name, die Anschrift, das Geburtsdatum und die Gültigkeitsdauer des Dokuments benötigt, vgl. auch Art. 5 Abs. 1 Buchst. c) DS-GVO (Datenminimierungsgrundsatz). Die für die Identitätsfeststellung erhobenen Daten unterliegen zudem einer strengen und zeitlich begrenzten Zweckbindung: Sie dürfen ausschließlich zur Identitätsprüfung verwendet werden, nicht aber in den Datenbestand der verantwortlichen Stelle einfließen. Mittels eines Aktenvermerkes (z. B. „Identität überprüft“) wäre der Identitätsprüfung nach Vorlage des Dokuments in der Regel genüge getan. Demgegenüber wäre der vorgenannte Datenminimierungsgrundsatz verletzt, wenn der Verantwortliche im Sinne von Art. 4 Ziff. 7 DS-GVO die Identität ausnahmslos mittels eines Ausweisdokuments überprüfen würde.

Die Verantwortlichen werden angehalten genau zu prüfen, wann die Identifizierung der betroffenen Person bei der Geltendmachung von Betroffenenrechten mittels eines Ausweises tatsächlich erforderlich ist. Bereits in unserem 34. Tätigkeitsbericht Datenschutz 2018, S. 16 ff. gehen wir detailliert auf die differenzierten Möglichkeiten einer Identitätsüberprüfung im Rahmen eines Auskunftsanspruchs nach Art. 15 DS-GVO ein.

5.4.4. Zeugenschutz und Anschriftennennung im Ermittlungsverfahren

Art. 57 Abs.1 Buchst. b) DS-GVO

Im Rahmen des polizeilichen und staatsanwaltschaftlichen Handelns werden von Zeug_innen im Ermittlungsverfahren regelmäßig Name und Wohnanschrift erhoben. Einige Zeug_innen haben daher Sorge, dass diese Angaben der beschuldigten Person bekannt werden, wenn dessen Verteidigung Akteneinsicht erhält. Der Beitrag stellt dar, wie die Interessen des Schutzes von Zeug_innen vor Beeinflussung, Einschüchterung oder Gefährdung mit dem Recht auf ein faires Verfahren des Beschuldigten in Einklang gebracht werden können.

Innerhalb eines strafrechtlichen Ermittlungsverfahrens im Sinne der Strafprozessordnung (StPO) gilt es, verschiedene Zielrichtungen miteinander in einen Ausgleich zu bringen: Zum einen ist der Strafprozess auf das Ziel der Wahrheitsfindung ausgerichtet und soll eine effektive Aufdeckung und Ermittlung von Straftaten ermöglichen. Zum anderen geht es im Strafprozess aber auch darum, gegenüber der beschuldigten Person ein rechtsstaatliches und faires Verfahren sicherzustellen. Hierzu gehört u.a., dass die Beschuldigten (ebenso wie die übrigen Prozessbeteiligten) nachvollziehen können, aufgrund welcher Beweislage den Beschuldigten welcher Tatvorwurf zur Last gelegt wird. Dabei müssen für ein rechtsstaatliches, faires Verfahren die Beschuldigten selbst in die Lage versetzt werden, die Beweise zu überprüfen und ggf. auch durch eigene Entlastungsbeweise zu erschüttern versuchen zu können (sog. Grundsatz der „Waffengleichheit“). Hierzu ist es insbesondere erforderlich, den Beschuldigten bzw. deren Verteidigung möglichst frühzeitig und möglichst umfassend Akteneinsicht zu gewähren. Zugleich hat der Staat bei der Regelung des Strafprozesses aber auch die Rechte Dritter zu berücksichtigen, etwa Zeugen nicht übermäßig zu belasten und vor rechtswidriger Beeinflussung oder gar Schädigung zu schützen. Diesen verschiedenen Interessen versucht der Strafprozess durch ein Geflecht von Regelungen Genüge zu leisten, die im Zusammenhang zu sehen sind.

Die Erfassung der vollständigen Wohnanschrift der Zeugin/des Zeugen ist Teil der Angaben zur Person und in der Vorschrift des § 68 StPO geregelt, die unmittelbar für die richterliche Vernehmung gilt, deren Grundzüge auch aber für die staatsanwaltschaftlichen (vgl. § 161a Abs.1 Satz 2 StPO) und polizeilichen Vernehmungen (vgl. § 163 Abs.3 Satz 2 StPO) im Rahmen des Strafprozesses gelten. Grundsätzlich müssen Zeug_innen innerhalb von Strafverfahren danach Angaben zum Namen, zu Alter und Beruf machen sowie ihre vollständige Anschrift nennen (§ 68 Abs.1 StPO). Diese Angaben dienen dazu, die aussagende Person eindeutig zu identifizieren und damit insbesondere Verwechslungen zu vermeiden. Zugleich sollen die Angaben aber auch eine belastbare Grundlage für die Beurteilung der Glaubwürdigkeit der Zeugenperson darstellen. Die Verfahrensbeteiligten erhalten dadurch insbesondere die Möglichkeit, Erkundigungen über Zeug_innen einzuholen oder Ladungen ordnungsgemäß zu bewirken (BeckOK StPO/Monka, 55. Ed. 1.4.2025, StPO § 68 Rn. 1). Zum Schutz der Zeug_innen wird in richterlichen Vernehmungen in Anwesenheit des Beschuldigten und in der Hauptverhandlung allerdings nicht die vollständige Anschrift, sondern nur dessen Wohn- oder Aufenthaltsort abgefragt, sofern nicht ausnahmsweise Zweifel über die Identität des Zeugen bestehen (§ 68 Abs.1 Satz 2 StPO). Außerdem können Zeug_innen, die Wahrnehmungen in amtlicher Eigenschaft gemacht haben, statt des Wohnortes ihren Dienstort angeben (§ 68 Abs.1 Satz 3 StPO).

Außerdem gilt: Wenn ein begründeter Anlass zu der Besorgnis besteht, dass durch die Angabe der vollständigen Anschrift Rechtsgüter der Zeugenperson oder einer anderen Person gefährdet werden oder dass auf Zeug_innen oder eine andere Person in unlaute-

Infokasten

„Die Auskunft im Sozialdatenschutz“, LfDI BW, 36. Tätigkeitsbericht Datenschutz 2020, S. 94ff.: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf

Übersicht: Zugangsrechte neben dem Landesinformationsfreiheitsgesetz BW (LIFG) unter: https://www.baden-wuerttemberg.datenschutz.de/zugangsrechte-neben-lifg/

rer Weise eingewirkt werden wird, soll einer Zeugin/einem Zeugen nach § 68 Abs. 2 StPO gestattet werden, statt der vollständigen Anschrift den Geschäfts- oder Dienstort oder eine andere ladungsfähige Anschrift anzugeben. Und wenn schon die Angabe des Wohn- oder Geschäftsortes eine entsprechende die Besorgnis hervorzurufen geeignet wäre (etwa weil mit Angabe des Ortes die genaue Anschrift ohne weiteres zu ermitteln wäre), soll bei richterlichen Vernehmungen in Anwesenheit von Beschuldigten und in der Hauptverhandlung der betreffenden Zeugin/dem betreffenden Zeugen sogar die Angabe des Geschäfts- oder Wohnorts erlassen werden (§ 68 Abs. 2 Satz 2 StPO).

Darüber hinaus greifen weitere Schutzmöglichkeiten, wenn ein begründeter Anlass zu der Besorgnis besteht, dass durch die Offenbarung der Identität oder des Wohn- oder Aufenthaltsortes einer Zeugin/eines Zeugen bestimmte Rechtsgüter der Zeugenperson oder einer anderen Person, nämlich Leben, Leib oder Freiheit des Zeugen, gefährdet werden könnten. In diesem Falle können der Zeugenperson weitere Angaben zur Person erlassen werden oder ihr sogar gestattet werden, das Gesicht bei der Vernehmung zu verhüllen (s. dazu § 68 Abs. 3 StPO).

Zudem regelt § 68 Abs. 5 StPO, dass, soweit einer Zeugenperson gestattet wurde, Daten nicht anzugeben, bei Auskünften aus und Einsichtnahmen in Akten sicherzustellen , dass diese Daten anderen Personen nicht bekannt werden, es sei denn, dass eine Gefährdung im Sinne der Absätze 2 und 3 ausgeschlossen erscheint. Insofern erhält trotz des grundsätzlich umfangreichen Akteneinsichtsrechts der Verteidigung (§ 147 StPO), das im Interesse der Waffengleichheit und Ermöglichung einer effektiven Verteidigung ein wesentliches Verfahrensrecht ist, auch die Verteidigung nicht stets die Anschrift der Zeug_innen.

Diese Regelungen des § 68 StPO hat der Gesetzgeber zuletzt durch das Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021 (BGBl. I S. 2099) nachgeschärft, um Unklarheiten der früheren Gesetzesfassung auszuräumen, und dabei den Zeugenschutz verbessert. Zugleich wurde mit dieser Gesetzesänderung klargestellt, dass schon in der Anklageschrift nicht deren vollständige Anschrift, sondern nur deren Wohn- oder Aufenthaltsort anzugeben ist, was zuvor umstritten und für die Praxis unklar war. Für die Angaben in der Anklageschrift gelten zudem weitere Ausnahmen, wenn es sich um dienstliche Zeug_innen handelt oder wenn bei Zeug_innen eine Gefährdungslage im Sinne von § 68 Abs. 2 oder 3 vorliegt (s. §200 Abs. 1 StPO).

Die Regelungen zum Schutz der Zeug_innen und der verletzten Personen werden noch durch weitere Bestimmungen unterstützt. So können Zeug_innen sich eines anwaltlichen Beistandes bedienen; unter besonderen Voraussetzungen kann ihnen sogar ein anwaltlicher Beistand durch das Gericht beigeordnet werden (§ 68b StPO, § 406 f. StPO). Verletzte können sich darüber hinaus auch einer psychosozialen Prozessbegleitung bedienen oder unter Umständen eine solche beigeordnet erhalten (§ 406g StPO). Darüber hinaus wird Zeug_innen an vielen Gerichten eine Begleitung durch Ehrenamtliche angeboten.

Leider haben viele Zeug_innen bislang noch keine umfassende Kenntnis über die dargestellten Schutzrechte: So ist bisher gesetzlich noch nicht sichergestellt, dass betroffene Zeugenpersonen tatsächlich von ihren rechtlichen Möglichkeiten im Rahmen des Strafverfahrens Kenntnis erlangen. Insoweit ist zwar in §§ 406i-406l StPO für Verletzte und ihre Angehörigen bzw. Erben vorgeschrieben, dass diese generell über die Rechte aus §§ 406d 406h StPO und weitere außerstrafprozessuale Befugnisse frühzeitig, schriftlich und möglichst verständlich zu belehren seien.

Es gilt bereits jetzt: Sollten Zeug_innen bereits im Rahmen des Ermittlungsverfahrens die Sorge haben, sich mit einer Aussage in Gefahr zu bringen, sollten sie hierüber offen mit der Polizei, der Staatsanwaltschaft oder einer anwaltschaftlichen Vertretung sprechen. Sind Zeug_innen beispielsweise besorgt und können sie einen Grund dafür angeben, dass sie oder z. B. Ihre Familienangehörige durch die Angabe ihrer Wohnanschrift gefährdet werden könnten, können sie – wie ausgeführt – darauf hinwirken, dass ihre vollständige Anschrift geheim gehalten wird (vgl. § 68 Abs. 2 StPO). Statt die private Wohnanschrift anzugeben können Zeug_innen dann ggf. auch eine andere Adresse angeben, an der sie zuverlässig erreicht werden können (z. B. die Adresse der anwaltschaftlichen Vertretung oder einer Opferhilfeeinrichtung).

Machen Zeug_innen von der Regelung des § 68 Abs. 2 StPO Gebrauch und haben eine andere ladungsfähige Anschrift angegeben, so wird die ursprünglich erfasste Wohnanschrift in allen Vorgangsbestandteilen der Ermittlungsakte geschwärzt und hierüber ein Vermerk angefertigt. Die Meldeadresse wird dann der Handakte der Staatsanwaltschaft beigefügt, welche jedoch nicht

Teil des Akteneinsichtnahmerecht ist. Um zu gewährleisten, dass die Wohnanschrift der Zeug_innen von Anfang an nicht in den Akten auftaucht, sollten Betroffene daher frühzeitig, also schon bei der Erstattung der Strafanzeige daran denken, einen entsprechenden Hinweis auf die Gefährdung aufnehmen zu lassen. Die Staatsanwaltschaft oder das Gericht prüft dann im Fortgang des Strafverfahrens, ob weiterhin eine Gefährdung besteht, und trifft auch die abschließende Entscheidung, ob ein Adressdatenschutz im Verlauf des gesamten Strafverfahrens gewährt werden kann und muss.

Wenn aufgrund bestimmter Tatsachen das Verhalten einer beschuldigten Person den dringenden Verdacht begründet, sie werde auf Mitbeschuldigte, Zeug_innen oder Sachverständige in unlauterer Weise einwirken oder andere zu einem solchen Verhalten veranlassen und deshalb die Gefahr droht, dass die Ermittlung der Wahrheit erschwert werde, käme zudem auch in Betracht, dass das Gericht ggf. einen Haftbefehl wegen Verdunkelungsgefahr erlassen kann (s. § 112 Abs. 2 Nr. 3 Buchst. b) und c) StPO) und ggf. weitere Beschränkungen für die Untersuchungshaft (wie z. B. eine Anordnung der Überwachung von Besuchen sowie Telekommunikation und Post, s. § 119 StPO) vorsieht. Falls der Verdunkelungsgefahr auch durch andere, für die beschuldigte Person weniger einschneidende Maßnahmen hinreichend begegnet werden kann, kann das Gericht einen solchen Haftbefehl auch unter entsprechenden Auflagen außer Vollzug setzen, § 116 StPO.

Schon jetzt enthält die StPO zahlreiche Schutzmaßnahmen, damit Name und Adressdaten von Zeug_innen nicht immer offenbart werden müssen.

5.4.5. Schulnoten in Google-Drive und auf eBay

Art. 57 Abs.1 Buchst. a) DS-GVO

Schulen befassen sich oftmals intensiv mit dem Datenschutz, wir beraten auch nach Kräften. Der Schutz ist in den Schulen besonders wichtig, weil es um die Daten von Kindern geht. Aber zum Glück gibt es Schulleitungen, die das erkannt haben und aufmerksam reagieren, wenn Schüler_innen-Daten auf nicht sicheren Ordnern abgelegt werden oder bei schulfremden Onlinediensten unbeabsichtig sichtbar werden. Von zwei bemerkenswerten Fällen wollen wir hier kurz berichten.

Alles für alle – so bitte nicht

Ein Lehrer hat im Berichtszeitraum die Daten seiner ganzen Klasse – Diagnosen, Lernkontrollen, Noten, Namen, persönliche Einschätzungen – in einem Google-Drive-Ordner abgelegt, auf den alle Eltern der Klasse zugreifen konnten. So ein Daten-Buffet für alle ist natürlich keine gute Idee.

Transparenz gegenüber den Eltern ist wichtig, aber nicht, wenn die ganze Klasse mitlesen kann – und schon gar nicht, wenn noch Google dabei ist. Das Kultusministerium empfiehlt auch, Daten zu verschlüsseln. Auch ist im Übrigen fraglich, ob die technischen und organisatorischen Maßnahmen bei der Nutzung von Google-Drive ausreichend sind, um personenbezogene Daten dort zu verarbeiten. Die Schulleitung hat in die-

Wenn man Bilder oder andere sensible Dokumente weitgehend offen ins Netz stellt, kann es schnell emotional werden. Bild: Fabrizio Matarese / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

sem Fall sofort reagiert, die Verwendung von Google-Drive untersagt, die Schulbehörde informiert und uns die Datenpanne gemeldet.

Klamotten, dies das – und Schulnoten auf eBay

Ein Verkauf auf eBay kann ein Datenschutzproblem verursachen. Wenn man Kleidung verkauft, macht man natürlich Fotos, damit die Interessierten sehen, was sie kaufen können. Dumm nur, dass darunter die Notenliste einer Grundschulklasse lag. Diese war zwar nicht zum Verkauf gedacht, aber trotzdem auf eBay sichtbar.

Auch hier hat die Schulleitung mit Hilfe des Datenschutzbeauftragten der Schule dank Beschwerden der Eltern schnell reagiert, das Bild gelöscht und eBay gebeten, es auch aus dem Anzeigenarchiv zu entfernen.

Die Schulleitung hat dann diese Gelegenheit genutzt, um das ganze Kollegium über den richtigen Umgang mit Schüler_innendaten zu informieren, und betont, dass auch der Zugriff von Familienmitgliedern auf diese Daten verhindert und die Daten sicher aufbewahrt werden sollten.

5.4.6. Arzttermine online

Art. 57 Abs.1 Buchst. a) DS-GVO

Ärztinnen und Ärzte organisieren inzwischen vermehrt die Vereinbarung von Praxisterminen über ihre Website. Das kann sehr praktisch sein für alle Beteiligten, aber dabei ist datenschutzrechtlich manches zu beachten. Falls eine Datenpanne vorliegt, sind auch die betroffenen Personen zu benachrichtigen.

Die Vereinbarung von Terminen online kann für Arztpraxen und Patient_innen von Vorteil sein: In Zeiten des Fachkräftemangels kann das Praxispersonal die für die Terminvergabe notwenige Zeit einsparen und sich um andere Aufgaben kümmern. Und den Patient_innen werden unter Umständen schier endlos scheinende Versuche erspart, das Praxispersonal telefonisch zu erreichen.

Allerdings ist bei der Einrichtung solcher Terminvergabetools datenschutzrechtlich einiges zu beachten, und zwar auch und insbesondere dann, wenn externe Dienstleistende eingebunden werden. Da dieses Thema zunehmend an Bedeutung gewinnt, hat die Datenschutzkonferenz ein Positionspapier herausgegeben, an dessen Erstellung wir mitgewirkt haben. Das Positionspapier enthält zahlreiche Hinweise für den Umgang mit Terminverwaltungsunternehmen im Bereich der Heilberufe.

Zu welchen weitreichenden Folgen Fehler bei der Konstruktion und dem Einsatz von Terminvergabetools führen können, wurde uns an einem konkreten Fall deutlich, auf den wir durch eine Beschwerde aufmerksam wurden. Auch wenn die Bearbeitung des Falls noch nicht abgeschlossen ist, lässt sich hierzu schon Folgendes ausführen:

Rund 20.000 Datensätze von Patientinnen und Patienten, die mittels des Terminvergabetools einer Arztpraxis um einen Termin gebeten hatten, waren hier in einer sehr schwach gesicherten Online-Plattform abgelegt worden. Die Datensätze enthielten dabei regelmäßig nicht nur den Terminwunsch, die Personalien und Kontaktdaten der Anfragenden, sondern auch die Beschwerden, wegen derer die betroffenen Personen um einen Termin nachgesucht hatten. Diese Angaben waren vorhanden, weil das auf der Homepage eingebundene Terminanfrage-Formular ausdrücklich nach den Beschwerden fragte, die den Anlass für den Terminwunsch bildeten. Die in der Datenbank abgelegten Anfragen umfassten dabei einen Zeitraum von mehreren Jahren. Auf die Plattform konnte man durch Anklicken eines Links zugreifen. Dieser Link wurde sodann bei Stellung einer Terminanfrage wohl versehentlich einer anfragenden Person per E-Mail zugesandt, so dass diese nicht nur auf ihren eigenen Eintrag in der Datenbank, sondern auf die gesamte Datenbank zugreifen konnte.

Infokasten

Datenschutz bei der Terminverwaltung durch Heilberufspraxen. Positionspapier zum datenschutzkonformen Einsatz von Dienstleistern für Online-Terminbuchungen und das Terminmanagement, vom 16. Juni 2025: https://www.datenschutzkonferenz-online.de/media/dskb/DSK-Beschluss_Positionspapier_Terminverwaltungsunternehmen.pdf

Wie konnte es soweit kommen? Es stellte sich bei unseren Untersuchungen bislang heraus, dass die Arztpraxis mit einem Dienstleister kooperierte, der die gesammelten Daten der vermeintlichen „Einfachheit halber“ in einem frei verfügbaren Online-Tool speicherte.

Dabei wurden wesentliche Grundregeln im Datenschutz übersehen, wie insbesondere die notwendige technische Absicherung der Datenverarbeitung nach Maßgabe von Art. 24 DS-GVO einschließlich einer hinreichenden Zugangssicherung.

Aber auch weitere bei Online-Tools zu beachtende Fallstricke führt der Sachverhalt vor Augen:

So ist es insbesondere – wie auch im Positionspapier der Datenschutzkonferenz dargelegt – nicht erforderlich, schon zum Zweck der Terminvergabe die Patientinnen und Patienten konkret nach ihren Krankheitssymptomen zu befragen. Hierbei handelt es sich um die besonders schützenswerte Kategorie von Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO und Art. 9 DS-GVO), deren Erhebung und weitere Verarbeitung besonderen Voraussetzungen unterliegt; die Einhaltung des Grundsatzes der Datenminimierung (Art. 5 Abs.1 Buchst. c) DS-GVO), dem zufolge die verarbeiteten Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein müssen, ist hier besonders wichtig.

Das Tool war außerdem, wie ausgeführt, so eingerichtet, dass die zu dem Zweck der Terminvereinbarung ins Formular auf der Website der Arztpraxis eingetragenen Daten auch Jahre später noch dort gelistet waren. Unter Umständen waren die betroffenen Personen gar nicht mehr Patient_innen der Arztpraxis. Hier hätte zumindest eine Löschroutine vorgesehen sein müssen, die die Löschung nicht mehr benötigter Daten nach einer bestimmten Zeit vorsieht. Der Zweck für die Datenspeicherung entfällt bei Terminvergabetools rasch, meist nach einigen Wochen: Sobald der in den Terminkalender eingetragene Termin verstrichen ist, besteht im Regelfall – wie in dem Positionspapier der Datenschutzkonferenz näher ausgeführt – keine Erforderlichkeit mehr, in dem Terminkalender weiterhin die Termindaten des Patienten oder der Patientin zu speichern, so dass sie dort zu löschen sind.

Aufgrund der Beschwerde und einer ersten Prüfung forderten wir die Arztpraxis umgehend auf, unverzüglich die Liste aus dem Netz zu nehmen, uns die im Rahmen einer Meldung nach Art. 33 DS-GVO erforderlichen Informationen zu übermitteln und die betroffenen Personen über den Vorfall zu informieren (Art. 34 DS-GVO). Die weitere Untersuchung des Falles dauert nun noch an.

5.4.7. Datenschutz trotz Zeitmangel in der Pflege

Art. 57 Abs.1 Buchst. a) DS-GVO

Im Pflegebereich ist die Einhaltung des Datenschutzes wegen der sensiblen zu verarbeitenden Informationen besonders wichtig. Trotz des hohen Zeitdrucks im Pflegebereich kann es auch hier gelingen, mit durchdachten technischen und organisatorischen Maßnahmen das erforderliche Datenschutzniveau sicherzustellen. Sollte es dennoch einmal zu einer Verletzung des Schutzes personenbezogener Daten kommen, hat der verantwortliche Pflegedienst an die Pflichten aus Art. 33 und 34 DS-GVO zu denken.

Immer wieder erreichen uns Datenpannenmeldungen aus dem Bereich der häuslichen Pflege. Gesellschaften und Organisationen, die mit der Versorgung der zu Pflegenden beauftragt werden, erstellen oftmals noch in Papierform Listen für die jeweiligen Arbeitstage und die zu Pflegenden. In diesem Jahr häuften sich die Meldungen von verschiedenen Diensten und Einrichtungen, die mit der Pflege von Bedürftigen betraut sind. Nicht selten wurden dann Einsatzpläne in Papierform bei der zuletzt versorgten Person in der Wohnung vergessen. Die jeweilige Pflegekraft bemerkte dies meist erst nach Verlassen der Räumlichkeiten in der nächsten Wohnung, wenn sie die Unterlagen für den nächsten Pflegetermin benötigte. In einigen Fällen entdeckten die betreuten Personen die bei ihnen vergessenen Unterlagen und meldeten sich beim Pflegedienst. In diesen Fällen liegt eine Datenpanne nach Art. 33 DS-GVO vor, da im Falle des Liegenlassens eine Verletzung

Infokasten

BIDIB-Schulungen zum Datenschutz: https://www.baden-wuerttemberg.datenschutz.de/bidib-veranstaltungen/

der Sicherheit der in den Einsatzplänen enthaltenen personenbezogenen Daten gegenüber der Kenntnisnahme durch unbefugte Dritte eingetreten ist (vgl. Art. 4 Nummer 12 DS-GVO). Denn Daten von zu pflegenden Personen sollten eigentlich nur dem Pflegepersonal bekannt sein. Beim Liegenlassen in einem fremden Haushalt besteht indes die nicht fernliegende Möglichkeit, dass andere Personen von der Pflegebedürftigkeit (und ggf. weiteren Umständen) einer dritten Person erfahren, ohne dass dies für die Pflege erforderlich wäre oder sonst ein Rechtsgrund für eine Übermittlung vorläge. Pflegedaten stellen dabei Gesundheitsdaten gemäß Art. 4 Nummer 15 DS-GVO dar und sind damit besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO, die innerhalb des Datenschutzrechtes einer gesteigerten Sorgfaltspflicht und strengeren Schutzmaßnahmen unterfallen.

Verantwortliche Stellen wie die Pflegeorganisationen müssen die ihnen bekannten Daten daher besonders sorgfältig verarbeiten. Mitunter kann es sich auch um Sozialdaten handeln. Diese unterliegen ebenfalls einem strengen Schutz, dem Sozialgeheimnis gemäß § 35 des Ersten Buchs des Sozialgesetzbuchs (SGB I). Wir raten daher Pflegediensten, die bestehenden Prozesse und Abläufe genau zu prüfen und ggf. zu verbessern. So können Datenpannen in der Zukunft vermieden und generell den Vorgaben des Datenschutzes Rechnung getragen werden.

Auch kann Digitalisierung helfen: Da eine zunehmende Zahl von Pflegediensten digitale Endgeräte im Rahmen der Hausbesuche für ihre Mitarbeitenden zur Verfügung stellt, könnten Pflegedienste auch darüber nachdenken, Besuchslisten in digitaler Form auf technischen Geräten zu verwenden. Die Geräte sind dann zu verschlüsseln und so einzurichten, dass der Zugriff auf die Daten nur nach hinreichend sicherer Authentifizierung möglich ist. So würde selbst bei einem vergessenen oder verloren gegangenen Tablet oder Laptop ein Zugriff auf die darauf befindlichen Daten der Pflegebedürftigen durch Unbefugte verhindert. Darüber hinaus lässt sich so auch eine Löschroutine einrichten, wie sie grundsätzlich für Verantwortliche verpflichtend ist, die dazu führt, dass die nicht mehr benötigten personenbezogenen Daten vom Gerät entfernt werden bzw. die Zugriffsmöglichkeit auf solche Daten beendet wird.

Insgesamt müssen die hierbei genutzten Systeme und Anwendungen nach dem Stand der Technik so ausgestaltet und so eingerichtet sein, dass sie einen hinreichenden Schutz gegen unbefugte Zugriffe und Angriffe von außen bieten. Dies und die Notwendigkeit der Verankerung datenschutzkonformer Abläufe sind Pflichten, die in Art. 25 DS-GVO verankert sind. Es handelt sich um die sogenannten technischen und organisatorischen Maßnahmen, die eine verantwortliche Stelle ergreifen muss und über die sie Rechenschaft ablegen können muss.

So fragen wir bei Datenpannen regelmäßig nach den vorgesehenen Prozessen für die von der Meldung betroffenen Vorgänge. Eine verantwortliche Stelle muss dann beschreiben können, welche Regelungen sie zur Sicherung datenschutzkonformer Datenverarbeitung getroffen hat. Oft erkennen wir, dass eine der häufigsten Ursachen für Datenpannen darin zu sehen ist, dass von den vorgesehenen Abläufen des Verantwortlichen abgewichen wurde. Daher sind auch regelmäßige Schulungen für Beschäftigte elementar. Diese sollen sicherstellen, dass die Beschäftigten die Regeln des Datenschutzes im Allgemeinen, aber auch die hausintern getroffenen Regelungen und Abläufe gut kennen. Nur so kann der Verantwortliche das Verständnis der Mitarbeitenden für datenschutzrechtliche Regelungen fördern und diese dahingehend sensibilisieren, geltenden Vorgaben einzuhalten und zu wahren.

Sollte es dennoch einmal zu einer unbefugten Offenlegung von Gesundheitsdaten durch Pflegedienste kommen, sind die Pflichten aus Art. 33 und 34 DS-GVO zu beachten: Der Verantwortliche hat wie bei allen Datenpannen die Pflicht, den Vorfall unverzüglich, spätestens innerhalb von 72 Stunden, der für ihn zuständigen Datenschutzbehörde zu melden. Sofern innerhalb von 72 Stunden noch nicht alle erforderlichen Umstände aufgeklärt werden konnten, sind die späteren Erkenntnisse nachzureichen.

Der Verantwortliche hat zu prüfen, was die Ursachen für die Datenschutz-Verletzung waren, was er zur Abmilderung von Nachteilen für die betroffenen Personen tun kann und inwieweit er zur Vermeidung weiterer Datenpannen seine technischen und organisatorischen

Infokasten

Unsere Meldeformulare für Datenpannen-Meldungen, Beratungswünsche und Beschwerde: https://www.baden-wuerttemberg.datenschutz.de/kontakt-aufnehmen/

Maßnahmen zum Datenschutz nachbessern muss, wozu insbesondere eine erneute Sensibilisierung von Beschäftigten gehören kann. Zu prüfen ist außerdem im Einzelfall, ob betroffene Personen zu informieren sind. Wir gehen bei Datenpannen im Bereich der Gesundheitsdaten in der Regel von einer Pflicht zur Benachrichtigung der betroffenen Person nach Art. 34 DS-GVO aus, weil hier regelmäßig eine erhöhte Gefährdung der Rechte und Freiheiten der betroffenen Personen gegeben ist. Daher ist eine Benachrichtigung aus unserer Sicht in der Regel geboten.

Bei Datenpannen muss der Verantwortliche prüfen, ob er die Betroffenen informieren muss.
Bild: FrankBoston-stock.adobe.com

5.4.8. Verfahrensbeistandschaft

Art. 57 Abs.1 Buchst. a), b), d), f) DS-GVO

Wenn Eltern und Familien vor dem Familiengericht um das Sorgerecht oder den Umgang ringen, braucht das Kind eine eigene Stimme. Genau zu diesem Zweck bestellt das Familiengericht Verfahrensbeistände. Kernaufgabe der Verfahrensbeistände ist es, das Interesse des Kindes festzustellen und im Verfahren zur Geltung zu bringen, das Kind altersangemessen über Gegenstand, Ablauf und möglichen Ausgang zu informieren und – wo sinnvoll – an einvernehmlichen Lösungen mitzuwirken. Im Rahmen der Tätigkeiten der Verfahrensbeistandschaft sind regelmäßig u.a. Gespräche mit Eltern und Bezugspersonen des Kindes zu führen, so dass sich hieraus zahlreiche datenschutzrechtliche Fragestellungen ergeben können.

In Kindschaftssachen ergänzen das Gesetz über das Verfahren in Familiensachen in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) und die Zivilprozessordnung (ZPO) die Vorgaben der DS-GVO um spezifische Regeln für das Familiengericht. Während für die Jugendhilfe das Achte und Zehnte Buch des Sozialgesetzbuches (SGB VIII und SGB X) den datenschutzrechtlichen Rahmen setzen, fehlen für Verfahrensbeistände bislang spezielle datenschutzrechtliche Regelungen für den Umgang mit personenbezogenen Daten. Daher gelten für sie die allgemeinen Bestimmungen der DS-GVO und des Bundesdatenschutzgesetzes (BDSG). Zahlreiche Beratungsanfragen von Eltern und Verfahrensbeiständen zeigen jedoch: Die Unsicherheit über die konkreten datenschutzrechtlichen Anforderungen ist groß. Dieser Beitrag klärt die wichtigsten, grundlegenden Fragen.

Verantwortlichkeit

Aufgabe der Verfahrensbeistände ist es, im familiengerichtlichen Verfahren das Interesse des Kindes festzustellen und im Verfahren zur Geltung zu bringen (§ 158b Abs.1 Satz 1 FamFG). Im erweiterten Aufgabenkreis, der ausdrücklich vom Gericht angeordnet werden muss (§ 158b Abs. 2 FamFG), kann es zudem für Verfahrensbeistände erforderlich sein, mit weiteren Bezugspersonen des Kindes zu sprechen, ausnahmsweise auch mit Bezugspersonen, die – wie beispielweise Lehrkräfte oder Erzieher_innen – in einer professionellen Beziehung zum Kind stehen. Dabei erheben Verfahrensbeistände personenbezogene Daten zum Zwecke der Wahrnehmung der subjektiven und objektiven Interessen des Kindes, der parteilichen Interessenvertretung des Kindes im Verfahren (Sicherstellung des Kindeswohls) und dazu, gegenüber dem Gericht Bericht zu erstatten, Stellung zu nehmen und den Sachstand mitzuteilen.

Nach Art. 4 Nr. 7 DS-GVO ist grundsätzlich jede „natürliche oder juristische Person, Behörde, Einrichtung oder anderer Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“, datenschutzrechtlich verantwortlich. Da Verfahrensbeistände selbstständig festlegen, welche Informationen und personenbezogenen Daten sie erheben und an das Gericht berichten möchten, sind sie als Verantwortliche anzusehen. Sie sind weder weisungsgebunden noch unterliegen sie der gerichtlichen Aufsicht (OLG Karlsruhe, Beschluss vom 4.7.2019 – 18 UF 62/19, NJW 2020, 411, Rn. 20). Sie sind insbesondere keine Auftragsverarbeiter des Gerichts, da sie keinen weisungsgebundenen „Auftrag“ zur Datenverarbeitung, sondern eine gesetzlich definierte Aufgabe zur eigenständigen Wahrnehmung erhalten.

Rechtsgrundlagen der Verarbeitung

Verfahrensbeistände verarbeiten regelmäßig personenbezogene Daten des Kindes, der Eltern und Dritter, darunter oft auch sensible Daten nach Art. 9 DS-GVO. Als zentrale Rechtsgrundlage dient Art. 6 Abs.1 Buchst.f) DS-GVO. Hiernach ist die Verarbeitung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen der betroffenen Person nicht überwiegen.

Die Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen stellen ein berechtigtes Interesse an der Verarbeitung der personenbezogenen Daten von betroffenen Personen dar. Hierbei werden neben den Interessen des Verantwortlichen auch Drittinteressen umfasst. Das berechtigte Interesse kann sich hierbei zunächst aus den Rechtsansprüchen der Eltern (als Dritte) ergeben, die den Rechtsstreit führen. Des Weiteren kann sich das Interesse aber aus den Rechten und Grundrechten des minderjährigen Kindes während des Prozesses ergeben, die einen für das Kind interessengerechten Ausgang des Verfahrens erfordern. Besteht ein berechtigtes Interesse, ist auf einer zweiten Stufe zu prüfen, ob die Datenverarbeitung zur Verwirklichung des festgestellten berechtigten Interesses erforder-

lich ist. Insbesondere dann, wenn die Interessen des Kindes im Verfahren nicht ausreichend durch die Eltern wahrgenommen werden können, ist es – nicht nur in den Fällen des § 158 Abs. 2 FamFG – regelmäßig nötig, eine Verfahrensbeistandschaft zu bestellen. Schließlich dürfen entgegenstehende Interessen betroffener Personen nicht überwiegen. Da die Verarbeitung von personenbezogenen Daten die Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen sowie die Rechte und Grundrechte des Kindes während des Verfahrens schützt, streitet in der Regel das hohe Gewicht der verfolgten Interessen für die Datenverarbeitung, so dass Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen das wahrgenommene berechtigte Interesse der Verfahrensbeistände überwiegen.

Werden im Rahmen der Verfahrensbeistandschaft besondere Kategorien personenbezogener Daten nach Art. 9 DS-GVO, z. B. Gesundheitsdaten, verarbeitet, ist zusätzlich ein Erlaubnistatbestand nach Art. 9 Abs. 2 DS-GVO nötig. Hier greift regelmäßig Art. 9 Abs. 2 Buchst. f) DS-GVO, da die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Herkunft der Daten und Verfahrensverzeichnis

Mit der Bestellung erhalten Verfahrensbeistände Akteneinsicht in das/die familiengerichtlich relevanten Verfahren. Innerhalb dieser Akten werden der Verfahrensbeistandschaft regelmäßig Name, Adresse, Telefonnummer, E-Mailadresse und weitere personenbezogene Daten (Familienverhältnisse, Wohnverhältnisse, außerfamiliäre Beziehungen, Gesundheit, Finanzen, Bildung, Strafverfahren u. w.) der Familienmitglieder bekannt. Weitere verarbeitete Daten können z. B. aus Gesprächen stammen, die dokumentiert werden. Bei einem erweiterten Bestellungsauftrag nach § 158b Abs. 2 FamFG führt die Verfahrensbeistandschaft Gespräche mit den Eltern und weiteren Bezugspersonen des Kindes.

Zur Erfüllung dieser Aufgaben sind Verfahrensbeistände befugt, zwecks Feststellung der Kindesinteressen personenbezogene Daten zu verarbeiten. Für die Datenerhebung bzw. Einholung von Auskünften bei Dritten bedürfen Verfahrensbeistände ggf. einer Schweigepflichtentbindung der gesetzlichen Vertreter des betroffenen Kindes. Im Rahmen seiner/ihrer eigenverantwortlichen und nicht der gerichtlichen Weisung unterworfenen Wahrnehmung der Aufgaben haben Verfahrensbeistände selbst zu entscheiden, mit welchen Dritten (z. B. Kindergarten, Schule, Arzt) sie sprechen.

Sämtliche Verarbeitungen sind nach Art. 30 DS-GVO in einem Verarbeitungsverzeichnis zu dokumentieren. Stets ist hierbei zu beachten, dass die Erhebung unter dem Gebot der Zweckbindung, der Transparenz, dem Prinzip der Datenminimierung, dem Grundsatz der Speicherbegrenzung wie auch der Integrität und Vertraulichkeit zu erfolgen hat. In den Berichten der Verfahrensbeistände an das Gericht sollten die jeweiligen Datenquellen klar aufgeführt werden und somit allen Verfahrensbeteiligten offenbart werden. In den zu erteilenden Datenschutzhinweisen müssen die aufgeführten Quellen personenbezogener Daten entsprechend vollständig aufgeführt werden.

Übermittlung personenbezogener Daten an Dritte

Eine Übermittlung personenbezogener Daten durch Verfahrensbeistände an Dritte ist nur mit einer entsprechenden Rechtsgrundlage oder Einwilligung der betroffenen Personen zulässig. Die Übermittlung an das Familiengericht stellt eine solche Übermittlung an Dritte dar. Weiterhin ist davon auszugehen, dass personenbezogene Daten im Rahmen der familiengerichtlichen Verfahren auch an Beschwerdegerichte und sonstige Verfahrensbeteiligte übermittelt werden. Diese Übermittlungen können ggf. auf Art. 6 Abs. 1 Buchst. f) DS-GVO gestützt werden. Auch bei Gesprächen mit Dritten kann es u. U. zu Übermittlungen kommen, soweit zur Interessenswahrnehmung erforderlich.

Einhaltung technisch-organisatorischer Maßnahmen nach Art. 32 DS-GVO

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet („Integrität und Vertraulichkeit"). Dieser Grundsatz des Art. 5 Abs. 1 Buchst. f) DS-GVO wird u.a. durch Art. 32 DS-GVO näher konkretisiert. Nach der Vorschrift haben Verantwortliche – also auch Verfahrensbeistände geeignete technische und organisatorische Maßnahmen (TOM) zu treffen Das Ziel ist ein Schutzniveau, das dem Risiko für die Betroffenen angemessen ist – unter Berücksichtigung von Stand der Technik und Implementierungskosten. Da viele Verfahrensbeistände nicht über gesonderte Geschäftsräumlichkeiten verfügen und im heimischen Arbeitszimmer tätig sind, ergeben sich besondere Anforderungen an die Arbeitsumgebung:

Verfahrensbeistände haben ihre Arbeitsumgebung so zu gestalten, dass Unbefugte keinen Zugriff und keine Kenntnis über personenbezogene Daten aus den betreuten Verfahren erhalten können, und zwar auch wenn den Beiständen keine geschäftlichen Büroräumlichkeiten zur Verfügung stehen. Verfahrensbezogene Unterlagen dürfen nicht offen, sondern müssen verschlossen und geschützt in einer separaten, gesondert abschließbaren Räumlichkeit oder in Schränken aufbewahrt werden. Der Arbeitsplatz ist so zu gestalten, dass Unbefugte (Familienangehörige, Nachbarn, Mitbewohner) keinen Einblick in Verfahrensunterlagen erhalten können. Gespräche und Telefonate sollten grundsätzlich in geschlossenen Räumlichkeiten stattfinden. Sollte in der Wohnung des Beistands ein Wechsel an einen solchen Rückzugsort nicht möglich sein, sollte ein Rückruftermin oder ein Gesprächstermin außerhalb des Wohnhauses vereinbart werden. Telefongespräche sollten zudem in Zeiten gelegt werden, in denen keine Störung durch Mitbewohnende oder Familienmitglieder zu erwarten ist.

Wo datenschutzrechtliche Spezialnormen fehlen, gelten datenschutzrechtliche Grundnormen und entscheidet Professionalität: Verfahrensbeistände haben als Verantwortliche das Kindes- und Elternwohl datenschutzkonform zu wahren, indem sie ihre Rolle klar verantworten, hinsichtlich ihrer Datenverarbeitung transparent vorgehen und schützende Maßnahmen konsequent umsetzen.

5.4.9. Gerichtsvollzieher – wer ist verantwortlich?

Art. 57 Abs.1 Buchst. a, c), d), f)

Gerichtsvollzieher_innen üben eine vielfältige Tätigkeit aus: Sie bewirken Zustellungen, können Wohnungen durchsuchen, Schuldner_innen und Angehörige des Hausstandes befragen und den Gläubiger_innen unterrichten, Vermögensauskünfte abnehmen, bewegliche Sachen pfänden und versteigern und vieles mehr. Dabei verarbeiten sie eine Vielzahl personenbezogener Daten. Doch wer ist datenschutzrechtlich für ihr Handeln verantwortlich, und inwieweit unterliegen sie der Aufsicht durch uns? Antwort: Gerichtsvollzieher_innen sind mithin keine Verantwortlichen im Sinne von Art. 4 Nummer 7 DS-GVO. Vielmehr ist ihr Handeln dem jeweiligen Amtsgericht als datenschutzrechtlich Verantwortlichen zuzurechnen. Sie üben auch keine justizielle Tätigkeit im Sinne von Art. 55 Abs. 3 DS-GVO aus.

Im Berichtszeitraum bat uns das Ministerium der Justiz und für Migration Baden-Württemberg um unsere Einschätzung zu den aufgeworfenen Fragen. Hintergrund der Frage war, dass Gerichtsvollzieher_innen der baden-württembergischen Justiz als Beamte des Landesdienstes jeweils einem Amtsgericht zugewiesen sind. Sind deswegen die Amtsgerichte oder die Gerichtsvollzieher_innen jeweils für sich datenschutzrechtlich verantwortlich? Ist ihre Arbeit als „justizielle Tätigkeit“ zu werten, die nach Art. 55 Abs. 3 DS-GVO nicht unserer Aufsicht unterliegt?

Maßgeblich für die Entscheidung über die datenschutzrechtliche Verantwortung ist die Regelung in Art. 4 Nummer 7 DS-GVO. Danach ist diejenige Person, Behörde oder Stelle Verantwortlicher, die über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Der Europäische Datenschutzausschuss (EDSA) geht hierzu in seinen Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DS-GVO (Version 2.0) davon aus, dass grundsätzlich jede Verarbeitung personenbezogener Daten durch Mitarbeitende im Tätigkeitsbereich einer Organisation unter der Kontrolle dieser Organisation erfolgt. Eine andere Sicht wäre unseres Erachtens nur gerechtfertigt, wenn ausnahmsweise die handelnde Person oder Stelle ganz unabhängig von der Organisationseinheit, der sie zugehört, handelt. Dies Betrachtung ist innerhalb der Gerichte gerechtfertigt, soweit eine einzelne Person oder ein Spruchkörper im Rahmen der – sogar verfassungsrechtlich garantierten – richterlichen Unabhängigkeit handelt. Im Rahmen dieser Unabhängigkeit dürfen im Interesse der Gewaltenteilung auch die Datenschutz-Aufsichtsbehörden keine Aufsichtsfunktion übernehmen, Art. 55 Abs. 3 DS-GVO. Aber sind die Gerichtsvollzieher_innen vergleichbar unabhängig in ihren Handlungen?

Nach § 1 der Gerichtsvollzieherordnung (GVO) handelt ein Gerichtsvollzieher bei der ihm zugewiesenen Zwangsvollstreckung selbstständig und unterliegt nicht der unmittelbaren Leitung des Gerichts. Die „Selbständigkeit“ erreicht aber nicht eine mit der richterlichen „Unabhängigkeit“ vergleichbare Qualität. Es existiert – anders als bei der verfassungsrechtlichen Garantie der Unabhängigkeit spruchrichterlicher Tätigkeit – keine gesetzliche Vorschrift, nach der Gerichtsvollzieher nur dem Gesetz unterworfen seien. Gerichtsvollzieher unterstehen vielmehr nach § 1 GVO

Infokasten

EDSA-Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf

der Aufsicht des Gerichts; unmittelbare_r Dienstvorgesetzte_r ist dabei der oder aufsichtführende Richter_in des Amtsgerichts. Als Beamten obliegt den Gerichtsvollzieher_innen eine Pflicht zu Gehorsam gegenüber ihrem Dienstherrn, die nach ständiger Rechtsprechung des Bundesverfassungsgerichts zu den hergebrachten Grundsätzen des Berufsbeamtentums gehört (vgl. BVerfG, Urteil vom 27. April 1959 – 2 BvF 2/58 – juris, Rn. 73).

In vielen Fällen dürften Gerichtsvollzieher_innen auch nur einen eingeschränkten Entscheidungsspielraum über die Zwecke der Datenverarbeitung haben: Die Zwangsvollstreckung erfolgt auf Grundlage eines vollstreckbaren Titels, nach Maßgabe der Anträge des Gläubigers und stark formalisierter Vorschriften. Gerichtsvollzieher_innen können im Wesentlichen weder den Zweck der Verarbeitung noch die grundlegenden Mittel der Verarbeitung ändern. Vielmehr sind sie verpflichtet, die ihnen übertragenen Aufgaben durchzuführen und können dabei nicht unabhängig von der Organisationseinheit „Amtsgericht“ handeln.

Letzteres ist auch zahlreichen Vorschriften zu entnehmen. So sieht z. B. § 10 GVO vor, dass die/der aufsichtsführende Richter_in der/dem Gerichtsvollzieher_in einen örtlich begrenzten Bereich zuweist. Zudem ist in § 22 Abs. 3 GVO geregelt, dass die Dienstaufsicht einen Zwangsvollstreckungsauftrag aus besonderen Gründen einem anderen als dem zuständigen Gerichtsvollzieher zuweisen kann. Darüber hinaus geht auch Ziffer 9.2 der Verwaltungsvorschrift des Justizministeriums über Zusatzbestimmungen zur Gerichtsvollzieherordnung davon aus, dass Gerichtsvollzieher_innen rechtzeitig vor Einsatzbeginn eines IT-Systems dem Dienstvorstand die für das Verzeichnis nach Art. 30 DS-GVO (das vom Verantwortlichen zu führen ist) erforderlichen Angaben mitzuteilen haben. In dieser Vorschrift wird somit offensichtlich davon ausgegangen, dass Gerichtsvollzieher_innen das Verzeichnis nach Art. 30 DS-GVO nicht selbst führen und daher auch nicht Verantwortliche sind. Auch sieht § 30a GVO vor, dass der Gerichtsvollzieher bei einer Datenpanne unverzüglich seinen unmittelbaren Dienstvorgesetzten und den Datenschutzbeauftragten des Amtsgerichts zu benachrichtigen hat. Sodann hat das Amtsgericht als Verantwortlicher (und nicht der Gerichtsvollzieher selbst) ggf. die Melde- und Benachrichtigungspflichten aus Art. 33 und 34 DS-GVO zu erfüllen.

Auch Praktikabilitätsgründe sprechen gegen die Annahme, Gerichtsvollzieher selbst als Verantwortliche im datenschutzrechtlichen Sinne zu sehen: Würde eine Verantwortlichkeit der Gerichtsvollzieher_in angenommen werden, wäre jede_r Gerichtsvollzieher_in verpflichtet, einen Datenschutzbeauftragten zu bestellen (vgl. Art. 37 Abs. 1 Buchst. a) DS-GVO).

Im Übrigen gehen in der täglichen Praxis unseres Hauses auch die Amtsgerichte selbst von ihrer datenschutzrechtlichen Verantwortung für die Tätigkeit der Gerichtsvollzieher_innen aus. So treten wir im Falle von Beschwerden gegen Gerichtsvollzieher_innen stets an die Amtsgerichte als verantwortliche Stelle heran oder verweisen z. B. betroffene Personen, die nach Art. 15 DS-GVO Auskünfte über ihre von einer/einem Gerichtsvollzieher_in verarbeiteten Daten erhalten möchten, an das für hier zuständige Amtsgericht. Dieses Vorgehen hat sich bewährt: Alle von uns angehörten Amtsgerichte haben sich stets im Einklang mit unserer Ansicht als verantwortliche Stelle für das Handeln der Gerichtsvollzieher_innen verstanden. Entsprechend erhielten wir stets die angeforderten Stellungnahmen.

5.5. Abteilung 4: Datenschutz in der Privatwirtschaft

Baden-Württemberg ist ein starker Wirtschaftsstandort mit enorm vielen Unternehmen, die hier ihren Sitz haben. Zudem ist Baden-Württemberg ein Land der Vereinskultur und Stiftungen. Unsere Fachleute aus dieser Abteilung befassen sich mit allen Fragen rund um die Wirtschaft und Vereine sowie den Beschäftigtendatenschutz und den Internationalen Datentransfer.

5.5.1. Sicherheitsüberprüfung von Beschäftigten

Art. 57 Abs.1 Buchst. b), d) DS-GVO

Beschäftigte, die während ihrer Tätigkeit Zugang zu sicherheitsrelevanten Informationen erhalten, müssen ggf. sicherheitsüberprüft werden. Dies gilt nicht nur für Beschäftigte öffentlicher Stellen, sondern auch für Beschäftigte privater Unternehmen, die von öffentlichen Stellen beauftragt werden. Dabei sind die Interessen der betroffenen Personen zu beachten. Hiermit waren wir im Jahre 2024 im Rahmen einer Beratungsanfrage befasst. Ein Unternehmen in Baden-Württemberg sollte, um einen Auftrag zu erhalten, seine Beschäftigten eine Sicherheitserklärung nach dem Sicherheitsüberprüfungsgesetz (SÜG) abgeben lassen.

In Baden-Württemberg richtet sich die Sicherheitsüberprüfung von Beschäftigten nach dem Landessicherheitsüberprüfungsgesetz (LSÜG). Auf Bundesebene besteht das Sicherheitsüberprüfungsgesetz des Bundes (SÜG). Nach § 2 Abs.1 SÜG bzw. LSÜG ist eine Person, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll (betroffene Person), vorher einer Sicherheitsüberprüfung zu unterziehen. Die Sicherheitsüberprüfung bedarf der Zustimmung der betroffenen Person in der gesetzlich vorgeschriebenen Form. Die Sicherheitsüberprüfung betrifft Personen, die nach den internen Planungen mit hoher Wahrscheinlichkeit eine sicherheitsempfindliche Tätigkeit ausüben werden. Dabei wird im Regelfall ein enger zeitlicher Zusammenhang in dem Sinne vorausgesetzt, dass die Tätigkeit unmittelbar nach dem positiven Abschluss des Sicherheitsüberprüfungsverfahrens übertragen wird (Däubler, in Däubler, SÜG, 1 Aufl. 2019, § 2 Rn 4). Was unter einer „sicherheitsempfindlichen Tätigkeit“ zu verstehen ist, findet sich in § 1 Abs.2 SÜG bzw. LSÜG. Es geht um Tätigkeiten, die den Zugang zu Verschlusssachen der Stufe STRENG GEHEIM, GEHEIM oder VS-VERTRAULICH ermöglichen und um Tätigkeiten in einem Bereich, der aufgrund des Umfanges und der Bedeutung dort anfallender Verschlusssachen von der jeweils zuständigen Behörde zum Sicherheitsbereich erklärt worden ist. Ebenfalls umfasst sind Tätigkeiten, die den Zugang zu Verschlusssachen über- oder zwischenstaatlicher Einrichtungen und Stellen ermöglichen, wenn die Bundesrepublik Deutschland, das Land Baden-Württemberg oder ein anderes Bundesland verpflichtet ist, nur sicherheitsüberprüfte Personen hierzu zuzulassen. Eine sicherheitsempfindliche Tätigkeit übt nach § 1 Abs.4 SÜG bzw. § 1 Abs.3 LSÜG auch aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen oder nach dem LSÜG auch an einer besonders gefahrenträchtigen Einrichtung beschäftigt ist oder werden soll (vorbeugender personeller Sabotageschutz). Nach Bundesrecht kommt noch die Beschäftigung an einer besonders sicherheitsempfindlichen Stelle des Geschäftsbereiches des Bundesministeriums der Verteidigung („Militärischer Sicherheitsbereich“) hinzu.

Personen, bei denen eine Sicherheitsüberprüfung durchzuführen ist, geben im ersten Schritt eine Sicherheitserklärung nach § 13 SÜG bzw. LSÜG ab. Diese ist das Ausgangsdokument für das gesamte Verfahren der Sicherheitsüberprüfung (Däubler, in Däubler, SUG, 1 Aufl. 019, §13 Rn 1). Welche personenbezogenen Daten hier konkret anzugeben sind, richtet sich gemäß § 13 SÜG bzw. LSÜG danach, ob eine einfache Sicherheitsüberprüfung nach § 8 SÜG bzw. LSÜG oder eine erweitere Sicherheitsüberprüfung nach § 9 bzw. 10 SÜG bzw. LSÜG erforderlich ist, sowie nach den in § 13 SÜG bzw. LSÜG aufgeführten Spezialregelungen.

Bei der einfachen Sicherheitsüberprüfung werden nach § 12 Abs.1 SÜG bzw. LSÜG die Angaben in der Sicherheitserklärung unter Berücksichtigung der Erkenntnisse der Verfassungsschutzbehörden des Bundes und der Länder bewertet und es wird eine unbeschränkte Auskunft aus dem Bundeszentralregister und dem Gewerbezentralregister und eine Auskunft aus dem zentralen staatsanwaltschaftlichen Verfahrensregister eingeholt. Weiterhin werden, soweit im Einzelfall erforderlich, bei ausländischen betroffenen Personen, die keine freizügigkeitsberechtigten Unionsbürger sind, Ersuchen um eine Übermittlung der nach § 3 Abs.1 und 2 Nummer 5, 6

und 9 des AZR-Gesetzes gespeicherten Daten gestellt. Es werden Anfragen nach Landesrecht an die Polizeidienststellen der Wohnsitze der betroffenen Person unter Beteiligung des Landeskriminalamtes, in der Regel beschränkt auf die letzten fünf Jahre, sowie an die in der Rechtsverordnung nach § 58 Abs.1 des Bundespolizeigesetzes bestimmte Bundespolizeibehörde, das Bundeskriminalamt und die Nachrichtendienste des Bundes gestellt. Es erfolgt eine Einsicht in erforderlichem Maße in öffentlich sichtbare Internetseiten zu der betroffenen Person, die nach Bundesrecht im Ermessen der Behörde steht. Nach Landesrecht findet auch eine Einsicht in den öffentlich sichtbaren Teil sozialer Netzwerke statt. Bei Auslandsaufenthalten von ununterbrochen längerer Dauer als sechs Monaten in den vergangenen fünf Jahren erfolgen Anfragen an ausländische Sicherheitsbehörden oder nach dortigem Recht für solche Anfragen zuständige öffentliche Stellen. Bei der erweiterten Sicherheitsüberprüfung nach § 12 Abs.2 SÜG bzw. LSÜG werden auch nach Bundesrecht Anfragen an die Polizeidienststellen der innegehabten Wohnsitze im Inland der betroffenen Person, in der Regel beschränkt auf die letzten fünf Jahre, gestellt und es findet eine Prüfung der Identität der betroffenen Person statt. Jetzt kann auch nach Bundesrecht in erforderlichem Maße in den öffentlich sichtbaren Teil sozialer Netzwerke Einsicht genommen werden. Bei der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen befragt die mitwirkende Behörde nach § 12 Abs.3 SÜG bzw. LSGÜ zusätzlich von der betroffenen Person in ihrer Sicherheitserklärung angegebene Referenzpersonen und weitere geeignete Auskunftspersonen, um zu prüfen, ob die Angaben der betroffenen Person zutreffen und ob tatsächliche Anhaltspunkte vorliegen, die auf ein Sicherheitsrisiko schließen lassen.

Eine einfache Sicherheitsüberprüfung erfolgt nach § 8 SÜG bzw. LSÜG bei Personen mit Zugangsmöglichkeit zu Verschlusssachen der Stufe VS-VERTRAULICH und bei Personen mit Tätigkeiten in zum Sicherheitsbereich erklärten Bereichen. Bei Personen mit Zugangsmöglichkeit zu als GEHEIM eingestuften Verschlusssachen oder zu einer hohen Anzahl von als VS-VERTRAULICH eingestuften Verschlusssachen findet nach § 9 SÜG bzw. LSÜG eine erweiterte Sicherheitsüberprüfung statt. Nach Bundesrecht kann stets von einer erweiterten Sicherheitsüberprüfung abgesehen werden, soweit die zuständige Stelle im Einzelfall nach Art und Dauer der Tätigkeit eine einfache Sicherheitsüberprüfung für ausreichend hält. Das LSÜG gestattet dies nur bei der Zugangsmöglichkeit zu einer hohen Anzahl von als VS-VERTRAULICH eingestuften Verschlusssachen. Eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlung nach § 10 SÜG bzw. LSÜG findet bei Personen statt, die Zugang zu als STRENG GEHEIM eingestuften Verschlusssachen erhalten sollen oder ihn sich verschaffen können, die Zugang zu einer hohen Anzahl von als GEHEIM eingestufter Verschlusssachen erhalten sollen oder ihn sich verschaffen können, und Personen, die bei Nachrichtendiensten des Bundes bzw. dem Landesamt für Verfassungsschutz oder Behörden, die nach Feststellung der Regierung Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wahrnehmen, tätig werden sollen. Soweit die zuständige Stelle im Einzelfall nach Art und Dauer der Tätigkeit eine einfache oder erweitere Sicherheitsüberprüfung für ausreichend hält, wird von der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlung abgesehen.

Die öffentliche Stelle, bei der die Beschäftigten tätig werden, erhebt deren personenbezogene Daten auf Grundlage von Art. 6 Abs.1 Buchst. e) DS-GVO i.V.m. den einschlägigen Vorschriften des SÜG bzw. LSÜG. Werden die Daten nicht von den betroffenen Personen direkt, sondern von deren Arbeitgeber_innen angefordert, weil diese von der öffentlichen Stelle beauftragt werden sollen und zur Erfüllung des Auftrags die Beschäftigten eine sicherheitsrelevante Tätigkeit ausüben, benötigen auch die Arbeitgeber_innen eine Grundlage zur Übermittlung der Daten. Wenn die Voraussetzungen für die Abgabe der Sicherheitserklärung vorliegen, kann die entsprechende Datenübermittlung auf Art. 6 Abs. 1 Buchst. b) DS-GVO gestützt werden, wenn sie zur Durchführung des Arbeitsverhältnisses erforderlich ist, da die Beschäftigten ihre vertraglich geschuldete Arbeitsleistung sonst nicht erbringen können. Gegebenenfalls ist auch Art. 6 Abs.1 Buchst. f) DS-GVO einschlägig, wenn das Interesse der Arbeitgeber_innen an dem Auftrag nicht von dem Interesse der betroffenen Beschäftigten überwogen wird, keiner Sicherheitsüberprüfung unterzogen zu werden Zu beachten ist, dass die Beschäftigten sich ausdrücklich und schriftlich damit einverstanden erklären müssen, den Fragebogen für die Sicherheitserklärung auszufüllen.

Auf die Materialien der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Thema Sicherheitsüberprufung weisen wir hin (https://www.bfdi.bund.de/DE/Buerger/Inhalte/SÜG/FAQ.html). Ein Unternehmen, das einen Auftrag erhält, für dessen Erteilung eine Sicherheitsüberprüfung der mit der Ausführung des Auftrags befassten Beschäftigten nötig ist, sollte sorgfältig prüfen, ob die Voraussetzungen für eine solche vorliegen.

5.5.2. Wie viele Daten braucht es zum Einkauf im Tafel-Laden?

Art. 57 Abs.1 Buchst. a), d), h) DS-GVO

Eine begrenzte Anzahl an Waren soll auf möglichst viele bedürftige Menschen verteilt werden. Wird die Entscheidung, wer berechtigt ist und wer nicht, datenschutzkonform getroffen?

Aufgrund einer Pressemitteilung eines Tafelladens sowie eines Hinweises aus der Bevölkerung sind wir darauf aufmerksam geworden, dass dieser ein digitales Einlasssystem einführen wollte. Hierbei sollte zum einen die Häufigkeit der Einkäufe erfasst werden, zum anderen aber auch weitergehende Informationen wie die Größe der zu versorgenden Familien oder die Herkunftsländer. Da es sich hierbei – gerade auch mit Blick auf die besondere Situation armutsbetroffener Personen – um sensible Daten handelt, sind wir auf den Verein zugegangen zwecks Aufklärung und etwaiger Unterstützung.

Im Einzelnen: Wir haben der Internetseite einer Stadt in Baden-Württemberg folgende Informationen zum Einlass-System eines Tafel-Ladens, der als Verein organisiert war, entnommen.

Um möglichst vielen Menschen eine Versorgungsmöglichkeit mit günstigen Lebensmitteln und Hygieneartikeln zu ermöglichen und da die Warenmenge nicht mehr für alle reicht und die wenigen gespendeten Waren gerecht verteilt werden müssen, soll die Anzahl der wöchentlichen Besuche pro Kunde begrenzt werden. Das neue Einlass-System soll die Mitarbeitende der Tafel im Hinblick darauf unterstützen. Zur Erleichterung der Eingangskontrolle wird jeder Tafelausweis mit einem Barcode versehen, der den Kunden registriert. Und jede Person wird einmal fotografiert, um später sicherzustellen, dass Ausweis und Person zusammengehören. Mit einem Barcode-Scanner wird erkannt, wie oft die Person in der Woche schon die Tafel besucht hat. Die neue Erfassung dient auch der Statistik (z. B. die Zahl der Personen, die Häufigkeit des Einkaufs, die Größe ihrer zu versorgenden Familien oder ihre Herkunftsländer). Der Barcode ermöglicht einen Überblick, wie viele aktive Kund_innen der Verein hat, bzw. wie viele der insgesamt ausgegebenen Tafel-Ausweise noch genutzt werden. Außerdem werden Doppel-Ausstellungen von Ausweisen unterschiedlicher Behörden sowie abgelaufene bzw. erneuerungsbedürftige Tafel-Ausweise erkannt.

Es stellten sich uns hier zahlreiche Fragen, z. B. um welche personenbezogenen Daten es sich im Einzelnen handelt, auf jeweils welcher Rechtsgrundlage sie verarbeitet werden (so sind an eine Einwilligung als Rechtsgrundlage in einem faktischen Abhängigkeitsverhältnis, dem eine Bedürftigkeit zugrunde liegt, hohe Anforderungen zu stellen), auf welche Art und mit welcher Erforderlichkeit sie jeweils wem bekanntgegeben werden oder was genau auf dem Barcode eincodiert ist. Was ist auf dem Ausweis abgedruckt oder beim Abscannen des Ausweises ersichtlich oder in Statistiken verarbeitet, wurden die Tafel-Kunden ausreichend informiert und welches Löschkonzept liegt vor? All diesen Fragen gingen wir im Einzelnen nach.

Unsere datenschutzrechtliche Überprüfung hat ergeben, dass

- die Verarbeitung von Namen und Geburtsdatum sowie Foto erforderlich sind. Sie dienen der Identifizierung und Sicherstellung, dass auch nur berechtigte Personen in der Tafel einkaufen
- die Rechtsgrundlage der Datenverarbeitung der Kundendaten überarbeitet werden musste
- der Verein die Datenschutzhinweise entsprechend unseren Hinweisen überarbeitet hat
- alle Ergebnisse statistischer Auswertungen anonymisiert sind
- eine Erfassung der gekauften Waren der jeweiligen Kunden nicht erfolgt
- keinerlei Information über die Bedürftigkeitsarten vorliegen und
- der Verein mit dem Dienstleister für die Software in Kontakt tritt, so dass keine Uhrzeit des Einkaufs mehr festgehalten wird, da diese Erhebung nicht erforderlich ist

Wir sehen einerseits die Schwierigkeiten in heutigen Zeiten für einen Verein, getragen von Ehrenamtlichen, Menschen in Not zu unterstützen. Andererseits ist Datenschutz Schutz von Grundrechten, gerade auch von bedürftigen Menschen, die auf bestimmte Dienstleistungen und Zuwendungen aus existenzieller Not angewiesen sind. Auch Informationen über das Einkaufsverhalten kann ein Bild über einen Menschen geben, das zu schützen ist. Wir konnten hier beiden Aspekten Rechnung tragen und am Ende dem Verein auch unterstützend unter die Arme greifen.

5.5.3. Bekanntgabe der Kündigungsgründe in der Belegschaft

Art. 57 Abs.1 Buchst. a), f) DS-GVO.

Bei uns häuften sich Beschwerden von Beschäftigten, die berichteten, dass die Gründe, aus denen sie gekündigt wurden oder selbst gekündigt hatten, innerhalb der Organisation der Arbeitgeber_innen preisgegeben wurden. Hierbei war zwischen verschiedenen Konstellationen zu unterscheiden:

1. Es wurde nur mitgeteilt, dass die beschäftigte Person gekündigt wurde bzw. selbst gekündigt hat. Gründe wurden nicht genannt. Teilweise wurde in diesem Zusammenhang beanstandet, dass die Kolleg_innen sogar vor der betroffenen Person über die Kündigung durch die Arbeitgeber_innen informiert wurden.

2. Es wurde mitgeteilt, dass die Kündigung aus betrieblichen Gründen, z. B. wegen Restrukturierungen, erfolgt ist.

3. Es wurde (mit unterschiedlichem Detaillierungsgrad) mitgeteilt, dass die Kündigung aufgrund mangelhafter Leistungen oder unzumutbaren Verhaltens der beschäftigten Person vorgenommen wurde. So hatte ein Arbeitgeber / eine Arbeitgeberin die Formulierung gewählt „Wir möchten Sie darüber informieren, dass aufgrund unüberbrückbarer Differenzen das Arbeitsverhältnis mit Frau XY frühzeitig beendet wird. Frau XY ist ab sofort freigestellt".

4. Es wurde mitgeteilt, dass die Kündigung aus gesundheitlichen Gründen erfolgt ist. Beispielsweise wurden die Kolleg_innen der betroffenen Person darüber informiert, dass diese mehrfach betrunken während der Arbeitszeit angetroffen wurde und man ihr Alkoholsucht unterstelle.

Teilweise waren die Arbeitgeber_innen der Meinung, zu diesem Verhalten berechtigt zu sein, um Gerede, z. B. Spekulationen über einen betriebsbedingten Personalabbau, zu beenden oder vorzubeugen. Es wurde von Arbeitgebendenseite auch vorgebracht, dass das Vermeiden dieser Spekulationen auch im Interesse der Person sei, die das Unternehmen verlassen habe, und diese Mitteilung dem Betriebsfrieden diene.

Arbeitgeber_innen haben ein berechtigtes Interesse daran, die Beschäftigten über das Ausscheiden von Mitarbeitenden zu informieren, da dies zur Fortführung des Geschäftsbetriebs notwendig ist. Die entsprechende Datenverarbeitung kann auf Art. 6 Abs.1 Buchst. b) oder f) DS-GVO gestützt werden. Jedoch dürfen nur die Informationen mitgeteilt werden, die zum unternehmensinternen Zweck erforderlich sind und die den Grundsatz der Datenminimierung aus Art. 5 Abs.1 Buchst. c) DS-GVO beachten. Dies betrifft die Information, dass und zu welchem Zeitpunkt eine beschäftigte Person das Unternehmen bzw. die Behörde verlässt. Über Umstrukturierungen dürfen die Beschäftigten auch dann informiert werden, wenn sie aus diesen zwangsläufig auf betriebsbedingte Kündigungen schließen können (z. B., weil alle Beschäftigten einer nun geschlossenen Abteilung betriebsbedingt gekündigt wurden).

Um durch das Ausscheiden einer beschäftigten Person ausgelöste Spekulationen über bevorstehenden weiteren Personalabbau und einer Neuorientierung von um ihren Arbeitsplatz fürchtenden Mitarbeitenden vorzubeugen, ist es ausreichend, über das Verlassen der jeweiligen beschäftigten Person zu informieren und gleichzeitig mitzuteilen, dass Restrukturierungen abgeschlossen sind und kein betriebsbedingter Personalabbau droht. Keinesfalls dürfen in diesem Zusammenhang, weder mündlich noch schriftlich, ohne deren Einwilligung die Gründe für die Kündigung der beschäftigten Person genannt werden. Teilweise waren Arbeitgeber_innen der Ansicht, dass mündliche Äußerungen datenschutzrechtlich nicht sanktioniert werden können. Zwar trifft zu, dass Datenverarbeitungen, die weder ganz oder teilweise automatisiert erfolgen noch Daten betreffen, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, nicht in den Anwendungsbereich der DS-GVO fallen, s. Art. 2 Abs.1 DS-GVO. Im Beschäftigtendatenschutz gilt jedoch für private Unternehmen § 26 Abs.7 Bundesdatenschutzgesetz. Danach liegt eine Datenverarbeitung auch vor, wenn personenbezogene Daten einschließlich besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Im öffentlichen Bereich gelten nach § 2 Abs.4 Satz 1 und 2 Landesdatenschutzgesetz (LDSG) die allermeisten Vorschriften der DS-GVO und das LDSG entsprechend für Datenverarbeitungen, die nicht in den Anwendungsbereich der DS-GVO oder der JI-Richtlinie fallen. Weder mündlich noch schriftlich dürfen insbesondere Gründe, die ehrenrührig sind oder

Bezug zu der gesundheitlichen Situation (z. B. krankhafter Alkoholkonsum) von Beschäftigten haben, ohne Einwilligung der betroffenen Person geäußert werden.

Arbeitgeber_innen müssen genau unter die Lupe nehmen, wann und wem gegenüber sie die Informationen, dass eine beschäftigte Person das Unternehmen bzw. die Behörde verlässt, bekannt geben dürfen.

Wenn Arbeitgeber_innen ihre gesamte Belegschaft über das Ausscheiden von Mitarbeitenden bereits zu einem Zeitpunkt informieren, in dem die Kündigung den Mitarbeitenden gegenüber selbst noch gar nicht zugegangen ist, legen sie ebenfalls personenbezogene Daten unzulässig offen. Ein Bedarf, über das Ausscheiden von Beschäftigten zu informieren, entsteht nämlich erst nach Zugang der Kündigung. Selbst wenn Arbeitgeber_innen mit „unüberbrückbaren Differenzen“ eine vergleichsweise neutrale Formulierung wählen und den konkreten Grund für die Kündigung nicht explizit benennen, ist eine solche Kommunikation geeignet, von Betroffenen als Beeinträchtigung des eigenen Ansehens wahrgenommen zu werden. Sie dürfte regelmäßig nicht erforderlich sein, um andere Mitarbeitende über das Ausscheiden der betroffenen Person zu informieren. Hier ist das Recht auf informationelle Selbstbestimmung der Beschäftigten gegenüber den betrieblichen Interessen der Arbeitgeber_innen vorrangig. Dies hatten wir gegenüber den jeweiligen Arbeitgebern, Dienstherren und Vorgesetzten, sowohl in der freien Wirtschaft wie auch im öffentlichen Dienst, klarzustellen und je nach Lage des Einzelfalls und insbesondere Sensibilität der veröffentlichten Informationen Verwarnungen auszusprechen.

5.5.4. Keine verpflichtende Zeiterfassung per Fingerabdruck

Art. 57 Abs.1 Buchst. a), f) DS-GVO

Im Jahre 2025 erreichte uns eine Beschwerde, wonach in einer Metzgerei in Baden-Württemberg die Zeiterfassung verpflichtend per Fingerabdruck erfolgte. Die verwendete Technologie speicherte dabei einen mathematischen Algorithmus des Fingerabdrucks (sog. Template). Die Datenerhebung wurde mit den Erfordernissen der Arbeitszeiterfassung begründet. Mit Blick auf die besondere Sensibilität der so erhobenen Daten galt es zu prüfen, inwieweit alternative und eingriffsärmere Methoden der Arbeitszeiterfassung den betrieblichen Anforderungen in gleichem Umfang gerecht würden.

Bild: Jamillah Knowles & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Personenbezogene Daten der Beschäftigten dürfen nur dann zur Arbeitszeiterfassung verarbeitet werden, wenn die Datenverarbeitung zu diesem Zweck erforderlich ist. Zunächst sind die Normen in den Blick zu nehmen, die das Unternehmen zur Arbeitszeiterfassung verpflichten. Für sämtliche Arbeitgeber_innen ergibt sich eine Rechtspflicht aus § 3 Abs. 2 Nr. 1 Arbeitsschutzgesetz (ArbSchG) in der Auslegung des Bundesarbeitsgerichts (s. BAG, Beschluss vom 13.09.2022 - 1 ABR 22/21 - BeckRS 2022, 25477). Für die dort genannten Unternehmen gilt auch § 17 Abs. 1 Mindestlohngesetz (MiLoG). Speziell die Fleischindustrie muss § 6 Abs. 1 Arbeitnehmerrechte-Sicherungsgesetz Fleischwirtschaft (GSA Fleisch) beachten.

Art. 6 Abs. 1 Buchst. c) Datenschutz-Grundverordnung (DS-GVO) in Verbindung mit § 3 Abs. 2 Nr. 1 ArbSchG in der Auslegung des Bundesarbeitsgerichts (s. BAG, Beschluss vom 13.09.2022 - 1 ABR 22/21 - BeckRS 2022, 25477) oder sonstigen zur Arbeitszeiterfassung verpflichtenden Normen erlaubt die Datenverarbeitungen, die erforderlich sind, um der Pflicht zur Arbeitszeiterfassung zu genügen. Hierbei ist zu berücksichtigen, dass das Bundesarbeitsgericht unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofs nur ein „objektives, verlässliches und zugängliches“ System verlangt, mit dem die von den Arbeitnehmer_innen geleistete tägliche Arbeitszeit gemessen werden kann. Wie dieses System konkret ausgestaltet ist, ist mangels einschlägiger gesetzlicher Regelungen den Arbeitgeber_innen, bzw. Arbeitgeber_innen und Betriebsrat, überlassen (BAG, Beschluss vom 13.09.2022 - 1 ABR 22/21 - BeckRS 2022, 25477, Rn. 65 mit Verweis auf EuGH, Urteil vom 14.05.2019 - C-55/18 – BeckRS 2019, 8402, Rn. 60 ff.). Eine Pflicht zur elektronischen Arbeitszeiterfassung ergibt sich aus § 3 Abs. 2 Nr. 1 Arbeitsschutzgesetz in der Auslegung des Bundesarbeitsgerichts nicht. Vielmehr führt das Gericht aus, dass – je nach Tätigkeit und Unternehmen – Aufzeichnungen in Papierform genügen. Zudem ist es, auch wenn die Einrichtung und das Vorhalten eines solchen Systems den Arbeitgeber_innen obliegt, nach den unionsrechtlichen Maßgaben nicht ausgeschlossen, die Aufzeichnung der betreffenden Zeiten als solche an die Arbeitnehmer_innen zu delegieren (BAG, Beschluss vom 13.09.2022 - 1 ABR 22/21 - BeckRS 2022, 25477, Rn. 65).

Auch zu § 17 Abs. 1 MiLoG bestehen keine näher bestimmten Anforderungen an die Form der Dokumentation der Arbeitszeit, sie kann auch an die Beschäftigten selbst übertragen werden (https://www.bmas.de/DE/Arbeit/Arbeitsrecht/Mindestlohn/Dokumentationspflicht/dokumentationspflicht.html; Greiner, in: BeckOK Arbeitsrecht, 76. Ed. 01.06.2025, § 17 MiLoG Rn. 5).

Es existiert auch ein Gesetzesentwurf des Bundesministeriums für Arbeit und Soziales aus dem Jahre 2023, der die Pflicht zur Arbeitszeiterfassung näher ausführt (s. die Zusammenfassung von Roloff, in: Erfurter Kommentar zum Arbeitsrecht, 25. Aufl. 2025, § 16 ArbZG Rn. 7). Hiernach sollen Arbeitgeber_innen verpflichtet werden, Beginn, Ende und Dauer der täglichen Arbeitszeit der Beschäftigten jeweils am Tag der Arbeitsleistung elektronisch aufzuzeichnen. Mitarbeitende können die Erfassung selbst vornehmen, Arbeitgeber_innen bleiben dann aber für die ordnungsgemäße Aufzeichnung verantwortlich und haben „durch geeignete Maßnahmen sicherzustellen“, dass ihnen „Verstöße gegen die gesetzlichen Bestimmungen zu Dauer und Lage der Arbeits- und Ruhezeiten bekannt werden.“ Der Entwurf sieht eine Informationspflicht der Arbeitgeber_innen vor: Sie müssen ihre Beschäftigten auf Verlangen über die aufgezeichnete Arbeitszeit informieren und ihnen ggf. eine Kopie der Aufzeichnungen zur Verfügung stellen. Die Aufzeichnungen sind für mindestens zwei Jahre aufzubewahren. Für Verstöße droht ein Bußgeld bis zu 30.000 Euro. Ob vergleichbare Regelungen jemals Gesetz werden, ist unklar.

Doch selbst eine Pflicht zur elektronischen Arbeitszeiterfassung verlangt keine Arbeitszeiterfassung über ein Fingerabdrucksystem. Neben den branchenübergreifend bereits gebräuchlichen Zeiterfassungsgeräten [Stechuhren mit Transpondern, Chips oder Stempelkarten, die die Arbeitszeit elektronisch speichern] kommen auch andere Formen der elektronischen Aufzeichnung mit Hilfe von digitalen Anwendungen in Betracht. Dabei kann die Eingabe in der digitalen Anwendung, wie etwa bei der Erfassung in einer Excel-Tabelle, auch manuell erfolgen (BR-Drs. 426/20, S. 34; für den oben dargestellten Gesetzesentwurf: Roloff, in: Erfurter Kommentar zum Arbeitsrecht, 25. Aufl. 2025, § 16 ArbZG Rn. 7). Ziel ist vor allem, behördliche Kontrollen und korrekte Zeiterfassung dadurch zu erleichtern, dass die Aufzeichnungen der Arbeitszeit in einer gut lesbaren und einer IT-gestützten Auswertung zugänglichen Form vorliegen (BR-Drs. 426/20, S. 34; Thüsing, in: BeckOK Arbeitsrecht, 76. Ed. 01.06.2025, § 6 GSA Fleisch Rn. 8 f.).

Art. 6 Abs. 1 Buchst. b) DS-GVO erlaubt die zur Durchführung des Arbeitsvertrags erforderlichen Daten-

verarbeitungen. Hier kann dem eigenen Interesse der Arbeitgeber_innen an der Arbeitszeiterfassung Rechnung getragen werden.

Biometrische Daten dürfen nur zur eindeutigen Identifizierung einer natürlichen Person verarbeitet werden, wenn einer der Fälle des Art. 9 Abs. 2 DS-GVO gegeben ist. Fingerabdrücke gehören zu diesen Daten, wobei es keine Rolle spielt, ob es sich um Rohdaten, also um exakte Abbildungen des Fingerabdrucks, oder um Templates handelt (Arning/Rothkegel, in: Taeger/Gabel, DS-GVO - BDSG – TTDSG, 4. Aufl. 2022, Art. 4 DS-GVO Rn. 398). Nach Art. 9 Abs. 2 Buchst. b) DS-GVO muss die Verarbeitung der Fingerabdrücke erforderlich sein, damit die Arbeitgeber_innen oder die beschäftigten Personen die ihnen aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und ihren diesbezüglichen Pflichten nachkommen können, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist.

Hieraus ergibt sich, dass eine Arbeitszeiterfassung über Fingerabdrücke oder andere biometrische Daten nur zulässig ist, wenn es keine andere Möglichkeit gibt, die den rechtlichen Anforderungen zur Arbeitszeiterfassung und den Anforderungen der Arbeitgeber_innen genügt und ohne die Verarbeitung biometrischer Daten auskommt.

Wir gehen davon aus, dass eine präzise und rechtssichere Arbeitszeiterfassung auch auf andere Weise als durch die Nutzung biometrischer Daten möglich ist, etwa durch Stempelkarten, Chips oder Transponder. Der Tatsache, dass Transponder, Chips oder Stempelkarten verloren gehen oder vergessen werden können, kann dadurch Rechnung getragen werden, dass die Beschäftigten aufgefordert werden, sorgfältig auf diese zu achten und sie stets zur Arbeit mitzubringen. Sollten Beschäftigte die Transponder, Stempelkarten oder Chips trotzdem vergessen oder verlieren, kann die Arbeitszeit für einen Übergangszeitraum von ihnen händisch bzw. in einer Excel-Tabelle erfasst werden. Dies wäre auch bei einer biometrischen Zeiterfassung ggf. nötig, wenn das System ausfällt. Ausführungen dazu, dass die Gefahr des Vergessens und Verlierens von Transpondern, Stempelkarten und Chips keine verpflichtende biometrische Arbeitszeiterfassung rechtfertigen kann, finden sich in LAG Berlin-Brandenburg, Urteil vom 04.06.2020 - 10 Sa 2130/19 - BeckRS 2020, 18964, Rn. 64.

Ob eine signifikante Gefahr besteht, dass Beschäftigte die Transponder, Chips oder Stempelkarten an Kolleg_innen weitergeben und diese für sich ein- oder ausstempeln lassen, wäre im konkreten Fall zu prüfen. Es dürfte in einem kleinen Betrieb u.a. Vorgesetzten und anderen Kolleg_innen sofort auffallen, wenn Beschäftigte während ihrer Arbeitszeit über längere Zeiträume nicht anwesend sind. Damit ist eine ausreichende Kontrolle gegen Arbeitszeitbetrug gewährleistet. Auf jeden Fall würde eine Nutzung von Systemen der biometrischen Zeiterfassung zur Verhinderung von Arbeitszeitbetrug voraussetzen, dass dokumentierte tatsächliche Anhaltspunkte vorliegen, dass es in dem Betrieb zum Ein- und Ausstempeln von Kolleg_innen füreinander kommt und dies nur durch eine biometrische Zeiterfassung verhindert werden kann (LAG Berlin-Brandenburg, Urteil vom 04.06.2020 - 10 Sa 2130/19 - BeckRS 2020, 18964, Rn. 70 ff.). Aufgrund der besonderen Sensibilität von Fingerabdrücken als biometrische Daten sind hieran hohe Anforderungen zu stellen.

Beispielsweise Lebensmittel verarbeitende Betriebe können Hygienevorschriften dadurch Rechnung tragen, dass die Beschäftigten Transponder, Chips bzw. Stempelkarten nicht offen herumliegen lassen, sondern diese während der Arbeit z. B. in Taschen oder Spinden verwahren.

Nach den obigen Ausführungen kommt eine Arbeitszeitüberwachung per Fingerabdruck nur in Betracht, wenn die Beschäftigten nach Art. 6 Abs. 1 Buchst. a) DS-GVO freiwillig in diese einwilligen. Dies setzt voraus, dass die Beschäftigten eine gleichwertige Alternative erhalten und nicht unter Druck gesetzt werden, sich für die Zeiterfassung per Fingerabdruck zu entscheiden. Das Unternehmen wird nunmehr den Beschäftigten eine Alternative zur Zeiterfassung per Fingerabdruck anbieten. Sollten sich die Beschäftigten trotzdem für die Zeiterfassung per Fingerabdruck entscheiden, wird dies dokumentiert. Damit konnten datenschutzkonforme Lösungen erarbeitet werden.

Arbeitgeber_innen sollten von Anfang an beachten, dass eine Arbeitszeiterfassung unter Verarbeitung biometrischer Daten in der Regel nur bei einer entsprechenden Einwilligung der Beschäftigten in Betracht kommt. Den Beschäftigten muss hierbei zumindest eine gleichwertige Alternative angeboten werden.

5.5.5. Abgleich der Daten von Beschäftigten mit Sanktionslisten (sog. „Terrorismuslisten“) – revisited

Art. 57 Abs.1 Buchst. b), d) DS-GVO

Der Sachverhalt, dass ein Unternehmen die Daten seiner Mitarbeitenden und von Bewerbenden automatisch mit sog. Sanktionslisten abgeglichen hat, war zuletzt im Jahre 2014/2015 Gegenstand unseres Tätigkeitsberichts. Sanktionslisten meint in diesem Zusammenhang Listen, die von der Europäischen Union (als Anhang zu Verordnungen) erstellt werden. Auf ihnen werden Personen und Organisationen aufgeführt, die von Maßnahmen zur Bekämpfung des Terrorismus betroffen sind und denen deshalb keine Gelder oder wirtschaftlichen Ressourcen zur Verfügung gestellt werden dürfen. Entsprechende Listen gibt es auch von den Vereinten Nationen, den USA und anderen Staaten. Im Jahre 2024 hat uns eine Beratungsanfrage veranlasst, das Thema erneut aufzugreifen.

Ein Abgleich der personenbezogenen Daten der Beschäftigten ist zum einen zur Erlangung des Status als Authorized Economic Operator (AEO) wichtig. Es handelt sich bei einem AEO um einen besonders zuverlässigen und vertrauenswürdigen Wirtschaftsbeteiligten. Die Zuverlässigkeit wird anhand der Einhaltung der zoll- und steuerrechtlichen Vorschriften, des Buchführungssystems, der Zahlungsfähigkeit und ggf. der Einhaltung von angemessenen Sicherheitsstandards bewertet. Der Status berechtigt zu Vergünstigungen bei sicherheitsrelevanten Zollkontrollen bzw. Vereinfachungen gemäß den Zollvorschriften (https://www.zoll.de/DE/Fachthemen/Zoelle/Zugelassener-Wirtschaftsbeteiligter-AEO/Allgemeines/allgemeines_node.html).

Der Bundesfinanzhof hat im Jahre 2012 entschieden, dass die Erteilung eines AEO-Zertifikats „Zollrechtliche Vereinfachungen/Sicherheit“ von der Bedingung abhängig gemacht werden darf, dass Antragstellende in sicherheitsrelevanten Bereichen tätige Bedienstete einer Sicherheitsüberprüfung anhand der sog. Terrorismuslisten der Anhänge der VO (EG) Nr. 2580/2001 und der VO (EG) Nr. 881/2002 unterziehen. In dem Urteil hat er ausgeführt, dass der entsprechende Datenabgleich zur Durchführung des Beschäftigungsverhältnisses erforderlich ist, wenn er dazu dient, bestimmte Erleichterungen bei der Abwicklung der unternehmerischen Tätigkeit, wie sie mit der Erteilung eines AEO-Zertifikats verbunden sind, zu erlangen. Dies sei der Fall, wenn diese Erleichterungen Sicherheitsvorkehrungen in Form einer Überprüfung des Personals des Verantwortlichen, das im sicherheitsrelevanten Bereich eingesetzt wird oder werden soll, erfordern (BFH, Urteil vom 19.06.2012 - VII R 43/11 – BeckRS 2012, 95804, Rn. 12 ff.). Weiterhin seien die Bediensteten durch einen bloßen Namensabgleich nur in geringem Umfang in ihrem Interesse am Schutz ihrer Privatsphäre betroffen, es würden wesentlich weniger Informationen offenbart als etwa in einem polizeilichen Führungszeugnis. Die betroffenen Personen würden auch nicht dem Verdacht ausgesetzt, ein potentieller Terrorist zu sein (BFH, Urteil vom 19.06.2012 - VII R 43/11 - BeckRS 2012, 95804, Rn. 12 ff.). Seit diesem Urteil kam die VO (EG) Nr. 753/2011 hinzu, mit der zur Erlangung des AEO-Status ebenfalls abzugleichen ist.

Wenn das Interesse von Arbeitgeber_innen am Erlangen des AEO-Status im konkreten Fall nicht von dem Interesse der Mitarbeitenden an dem Unterbleiben des Abgleichs überwogen wird, ist der Abgleich der Stammdaten der Mitarbeitenden mit den Listen in den Anhängen der genannten Verordnungen nach Art. 6 Abs.1 Buchst. f) DS-GVO zulässig. Maßgebliches Kriterium ist, inwieweit das Unternehmen bei seiner Geschäftstätigkeit mit Zollkontrollen zu tun hat und zur Aufrechterhaltung seiner Wettbewerbsfähigkeit den AEO-Status benötigt (vgl. LfDI Rheinland-Pfalz, Tätigkeitsbericht zum Datenschutz 2019, S. 45). Dies gilt allerdings nur für die in sicherheitsrelevanten Bereichen tätigen Beschäftigten. Die personenbezogenen Daten von Bewerbenden oder sonstigen Mitarbeitenden dürfen nicht zur Aufrechterhaltung oder Erlangung des AEO-Status mit Sanktionslisten abgeglichen werden. Art. 6 Abs.1 Buchst. b) DS-GVO wäre keine geeignete Rechtsgrundlage, wenn es um die Erlangung eines AEO-Status geht. Das Arbeitsverhältnis mit den betroffenen Beschäftigten kann zumindest in der Regel auch durchgeführt werden, ohne dass das Unternehmen den AEO-Status erlangt. Durch diesen wird lediglich der mit Zollkontrollen für das Unternehmen einhergehende Aufwand reduziert.

Weiterhin ist zu beachten, dass nach Art. 2 Abs.1 Buchst. b) der VO (EG) Nr. 2580/2001 und Art. 2 Abs. 2 der VO (EG) Nr. 881/2002 den in den Anhängen der Verordnungen genannten natürlichen oder juristischen Personen, Gruppen oder Organisationen weder Gelder

oder andere finanzielle Vermögenswerte noch wirtschaftliche Ressourcen direkt oder indirekt zur Verfügung gestellt werden oder zugutekommen dürfen. Das Gleiche gilt nach Art. 3 Abs. 2 der VO (EG) Nr. 753/2011 für die im Anhang zu dieser Verordnung genannten natürlichen und juristischen Personen. Unter dieses Bereitstellungsverbot fällt auch die Auszahlung von Arbeitsentgelten.

Damit können Arbeitgeber_innen ihrer arbeitsvertraglichen Pflicht zur Auszahlung des Arbeitsentgelts an die Mitarbeitenden nur nachkommen, ohne dabei einen Verstoß gegen ihre Pflichten aus diesen Verordnungen zu riskieren, wenn sie einen Abgleich der Stammdaten der Mitarbeitenden mit den Anhängen der Verordnungen (EG) Nr. 2580/2001, (EG) Nr. 881/2002 und (EG) Nr. 753/2011 vornehmen. Eine fahrlässige Verletzung des Bereitstellungsverbots ist nach § 19 Abs. 1 Nr. 1 i. V. m. § 18 Abs. 1 Nr. 1a AWG eine Ordnungswidrigkeit und kann nach § 19 Abs. 6 AWG mit einem Bußgeld bis zu 500.000 Euro sanktioniert werden. Fahrlässigkeit ist gegeben, wenn Arbeitgeber_innen pflichtwidrig Kontrollen unterlassen, ob ihre Beschäftigten auf Sanktionslisten stehen. Wer als Inhaber_in eines Betriebes oder eines Unternehmens vorsätzlich oder fahrlässig die Aufsichtsmaßnahmen unterlässt, die erforderlich sind, um in dem Betrieb oder Unternehmen Zuwiderhandlungen gegen Pflichten zu verhindern, die Inhabende treffen und deren Verletzung mit Strafe oder Geldbuße bedroht ist, handelt nach § 130 OWiG ordnungswidrig, wenn eine solche Zuwiderhandlung begangen wird, die durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.

Eine Aufsichtsmaßnahme, um Verstöße gegen die Pflicht zur Einhaltung des Bereitstellungsverbots zu verhindern, ist ein Personalabgleich mit den Sanktionslisten. Wird er unterlassen, besteht daher ein Bußgeldrisiko, wenn es zu einem Verstoß gegen das Bereitstellungsverbot kommt (Byers, Mitarbeiterkontrollen, 2022, S. 157; LfDI BW, 32. Tätigkeitsbericht Datenschutz 2014/2015, S. 146). Damit kann der Abgleich der Stammdaten der Mitarbeitenden mit den Anhängen der Verordnungen (EG) Nr. 2580/2001, (EG) Nr. 881/2002 und (EG) Nr. 753/2011 als zur Durchführung des Arbeitsvertrags nach Art. 6 Abs. 1 Buchst. b) DS-GVO erforderlich angesehen werden. Die Erforderlichkeit kann nicht deshalb abgelehnt werden, weil Banken vor dem Durchführen der Überweisung des Entgelts auf das Konto der Arbeitnehmenden ebenfalls einen Abgleich mit den genannten Listen durchführen. Arbeitgeber_innen haben keine Möglichkeit, zu kontrollieren, ob die Banken einen entsprechenden Abgleich tatsächlich durchführen und müssten sich ein entsprechendes Unterlassen der Banken zurechnen lassen (s. LfDI BW, 32. Tätigkeitsbericht Datenschutz 2014/2015, S. 146). Da damit Arbeitgeber_innen ihrer Pflicht zur Entgeltfortzahlung nur dann ohne Bußgeldrisiko nachkommen können, wenn sie den Abgleich mit den genannten Sanktionslisten vornehmen, ist dies zur Durchführung des Beschäftigungsverhältnisses bzw. des Arbeitsvertrags erforderlich nach Art. 6 Abs. 1 Buchst. b) Var. 1 DS-GVO. Bei Bewerbenden ist die Information, ob ihnen bei einer Einstellung ohne Bußgeldrisiko Gehalt ausgezahlt werden kann, für die Einstellungsentscheidung relevant. Haben sich die Verantwortlichen für eine bewerbende Person entschieden, kann bei dieser ein Abgleich mit den genannten Sanktionslisten auf Art. 6 Abs. 1 Buchst. b) Var. 2 DS-GVO gestützt werden. Er ist dann zur Durchführung des Bewerbungsverfahrens erforderlich, damit niemand eingestellt wird, dem letztlich kein Gehalt gezahlt werden darf.

Aus den oben dargestellten Erwägungen erachten wir einen Abgleich der Stammdaten der Beschäftigten mit den Anhängen der Verordnungen (EG) Nr. 2580/2001, (EG) Nr. 881/2002 und (EG) Nr. 753/2011 für datenschutzrechtlich zulässig. Die Argumentation, dass die Verordnungen selbst keine ausreichend bestimmte Rechtsgrundlage für den Datenabgleich erhält und diesen nicht verlangt, führt nach den obigen Erwägungen nicht zur Unzulässigkeit des Abgleichs. Mit der Frage,

Infokasten

N 29 2014, E-VSF-Nachrichten, 121; Allgemeines Zollrecht / Änderung der Dienstvorschrift „Zugelassener Wirtschaftsbeteiligter - AEO“ (E-VSF Z 05 20): https://www.datenschutz-notizen.de/wp-content/uploads/2015/01/E-VSF-N292014121.pdf

Hinweise zum Fragebogen für zollrechtliche Bewilligungen (AEO): https://www.zoll.de/DE/Fachthemen/Zoelle/Zugelassener-Wirtschaftsbeteiligter-AEO/Antragsverfahren/Hinweise-Fragebogen-zollrechtliche-Bewilligungen/hinweise-fragebogen-zollrechtliche-bewilligungen_node.html

ob eine Rechtsgrundlage außerhalb der Verordnungen (EG) Nr. 2580/2001, (EG) Nr. 881/2002 und (EG) Nr. 753/2011 existiert, hat sich der Düsseldorfer Kreis nicht beschäftigt.

Ein Abgleich der Mitarbeitendendaten mit anderen Sanktionslisten muss im konkreten Fall beurteilt werden. Entscheidend sind die Konsequenzen, die ein unterlassenes Screening für das betroffene Unternehmen nach sich ziehen kann, und ob es um Sanktionslisten in unmittelbar geltenden Rechtsakten der Europäischen Gemeinschaften oder der Europäischen Union geht, die ein Bereitstellungsverbot enthalten (s. z. B. https://www.zoll.de/DE/Fachthemen/ Aussenwirtschaft-Bargeldverkehr/Embargomassnahmen/ embargomassnahmen_node.html).

Der Abgleich muss verhältnismäßig ausgestaltet werden, er ist auf das unbedingt erforderliche Maß zu beschränken. Abgeglichen werden dürfen ausschließlich diejenigen Daten, die zur eindeutigen Identifizierung eines Beschäftigten zwingend notwendig sind. Dies sind in aller Regel der Vor- und der Nachname. Weitere Daten dürfen nicht abgeglichen werden. Weiterhin muss ein ausreichend großes Intervall zwischen den einzelnen Abgleichen gewählt werden, genannt wird ein jährlicher Abgleich (s. LfDI Rheinland-Pfalz, Tätigkeitsbericht zum Datenschutz 2019; S. 45; Byers, Mitarbeiterkontrollen, 2022, S. 159 f.). Der Abgleich muss den betroffenen Mitarbeitenden und Bewerbenden vorher mitgeteilt werden, die Informationspflichten des Art. 14 DS-GVO sind zu erfüllen. Der betriebliche Datenschutzbeauftragte muss in das Verfahren einbezogen werden.

Hinsichtlich der zu dem Abgleich eingesetzten Software muss diese, bzw. der Anbieter, hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass der Abgleich im Einklang mit den Anforderungen der DS-GVO erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet ist (vgl. Art. 28 Abs. 1 DS-GVO). Technische und organisatorische Maßnahmen nach Art. 24, 25 und 32 DS-GVO müssen getroffen werden, insbesondere muss ein Zugriff unbefugter Personen auf die verarbeiteten personenbezogenen Daten vermieden werden. Ein Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO muss mit dem Anbieter der Software abgeschlossen werden.

Wesentliche Rechtfertigung für den Abgleich der erforderlichen personenbezogenen Daten von Mitarbeitenden und Bewerbenden mit Sanktionslisten ist das Interesse an der Erlangung eines AEO-Status und daran, nicht verbotener Weise einer auf einer der Listen stehenden Person Gehalt zu zahlen und damit eine Ordnungswidrigkeit zu begehen. Jedoch ist es wichtig, bei der Durchführung dieser Abgleiche den Datenschutz, insbesondere den Erforderlichkeitsgrundsatz, zu beachten.

5.5.6. Tücken bei der Mitarbeitendenbefragung

Art. 57 Abs. 1 Buchst. a), f) DS-GVO

Uns erreichte eine Beschwerde über die Durchführung einer Mitarbeitendenbefragung bei einem Unternehmen in Baden-Württemberg.

Bei dem Unternehmen fand im Jahr 2024 eine Befragung der Mitarbeitenden über ihre Zufriedenheit mit ihrer Arbeit statt, mit deren Durchführung ein Dienstleister als Auftragsverarbeiter nach Art. 4 Nummer 8 und Art. 28 DS-GVO beauftragt worden war. Zur Durchführung der Mitarbeitendenbefragung gab das Unternehmen an den Dienstleister vorab eine Vielzahl über Kontaktdaten hinausgehende personenbezogene Stammdaten der Beschäftigten weiter, wie z. B. Geschlecht, Altersgruppe oder Beschäftigungsort. Dies geschah noch bevor die Beschäftigten die Gelegenheit hatten, eine Einwilligung zur Teilnahme an der Mitarbeitendenbefragung zu erteilen. Die elektronische Erteilung der Einwilligung in die Teilnahme an der Umfrage erfolgte erst unmittelbar bevor die Beschäftigten auf den Fragebogen gelangten und diesen ausfüllten. Mit Hilfe der Stammdaten sollten die Ergebnisse der Umfrage ausgewertet werden und es sollten Rückschlüsse darauf gezogen werden, welche Beschäftigtengruppen mit den Arbeitsbedingungen bei dem betroffenen Unternehmen zufrieden sind und welche nicht. Ziel war es, auf Basis dieser Erkenntnisse zielgruppenspezifische Maßnahmen zur Verbesserung der Arbeitsbedingungen zu entwickeln und umzusetzen.

In Vorbereitung auf die Mitarbeitendenbefragung wurde eine Informationskampagne mit dem Ziel gestartet, die Beschäftigten zur Teilnahme zu motivieren, insbesondere durch E-Mails und Videobotschaften von hochrangingen Beschäftigten des Unternehmens. Im Rahmen der Informationskampagne wurde unter ande-

rem ausgeführt, dass die Antworten anonym seien. Das Unternehmen erhalte nur aggregierte und dadurch anonymisierte Daten, insbesondere würden keine Antworten weitergegeben, wenn weniger als fünf Personen eine Frage beantwortet hätten.

Tatsächlich wurde getrackt, welche Beschäftigten an der Mitarbeitendenbefragung teilgenommen hatten, um eine hohe Beteiligungsrate zu erreichen.

Bei einem Beschäftigten, der ein Löschersuchen gestellt und sich bei uns über die Durchführung der Umfrage beschwert hatte, wurden die personenbezogenen Daten aus den Systemen zur Mitarbeitendenbefragung gelöscht.

Im vorliegenden Fall bestand keine Rechtsgrundlage nach Art. 6 Abs.1 DS-GVO für die Verarbeitung der personenbezogenen Daten der Beschäftigten im Zusammenhang mit der Mitarbeitendenbefragung. Art. 6 Abs.1 Buchst. b) DS-GVO, wonach die Datenverarbeitung zur Durchführung des Arbeitsvertrags erforderlich sein muss, ist für Mitarbeitendenbefragungen nur einschlägig, wenn die Antworten auf die gestellten Fragen zur Durchführung des Beschäftigungsverhältnisses nötig sind. Dies ist z. B. bei Fragen nach der allgemeinen Zufriedenheit und sozialen Kontakten im Unternehmen nicht der Fall. Sowohl Arbeitgebende als auch die Beschäftigten können ihren arbeitsvertraglichen und arbeitsrechtlichen Pflichten nachkommen, ohne dass die Antwort auf diese Fragen erhoben wird.

Die Durchführung der Umfrage in der praktizierten Form konnte auch nicht auf Art. 6 Abs.1 Buchst. a) bzw. f) DS-GVO gestützt werden.

Die Verarbeitung der personenbezogenen Daten im Vorfeld der Umfrage war nicht nach Art. 6 Abs. Buchst. f) DS-GVO zur Wahrung der berechtigten Interessen des Unternehmens oder eines Dritten erforderlich. Eine Verarbeitung der über die zur Einholung des Einverständnisses nötigen Kontaktdaten hinausgehenden Stammdaten der Beschäftigten durch den Dienstleister zwecks Auswertung der Ergebnisse der Umfrage hätte von vornherein erst nach deren Einwilligung in die Teilnahme an der Befragung vorgenommen werden dürfen, da es vorher hierfür keine Notwendigkeit gab. Zudem hat der EuGH entschieden, dass Art. 6 Abs.1 Buchst. f) DS-GVO dahin auszulegen ist, dass eine Verarbeitung nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich im Sinne dieser Vorschrift angesehen werden kann, wenn der Verantwortliche den Nutzenden ein mit der Datenverarbeitung verfolgtes berechtigtes Interesse mitgeteilt hat (GRUR-RS 2023, 15772, Rn. 126). In jedem Fall ist im Rahmen der Interessenabwägung auch die Transparenz der Verarbeitung zu berücksichtigen, vgl. Erwägungsgrund 47. Den Beschäftigten war nach dem Ergebnis des Beschwerdeverfahrens nicht mitgeteilt worden, dass bereits zur Vorbereitung der Mitarbeitendenbefragung über die Kontaktdaten hinausgehende personenbezogene Daten an den die Befragung durchführenden Dienstleister gegeben werden.

Die Einwilligung der teilnehmenden Beschäftigten nach Art. 6 Abs.1 Buchst. a) DS-GVO in die mit der Mitarbeitendenbefragung als solcher einhergehenden Datenverarbeitungen war nicht wirksam. Um wirksam zu sein, muss eine Einwilligung nach Art. 4 Nummer 11 DS-GVO insbesondere in informierter Weise erfolgen und freiwillig abgegeben werden. Es fehlte an der notwendigen Freiwilligkeit der Einwilligung der Beschäftigten in die Teilnahme an der Mitarbeitendenbefragung und die mit dieser einhergehenden Datenverarbeitungen. Da kontrolliert wurde, wer an der Umfrage teilnimmt, bestand die Gefahr, dass sich Beschäftigte unter Druck gesetzt fühlen, an der Umfrage teilzunehmen und in die damit verbundenen Datenverarbeitungen einzuwilligen oder berufliche Konsequenzen bei einer Nichtteilnahme zu befürchten haben. Dies galt auch vor dem Hintergrund der firmeninternen Werbekampagne für die Mitarbeitendenbefragung und der Zielvorgabe einer hohen Teilnahmequote.

Die Einwilligung der Beschäftigten war zudem nicht informiert im Sinne von Art. 4 Nummer 11 DS-GVO. Ihnen wurden wesentliche Informationen vorenthalten und sie wurden im Gegenteil mit verschiedenen Aussagen zur vermeintlichen Anonymität unzutreffend informiert. Es fehlten Datenschutzhinweise zur Umfrage, die die Anforderungen nach Art. 13 DS-GVO erfüllen. Diese hätten sowohl (a) über die selbst vom Beschäftigten durchzuführenden Angaben in den Fragebögen, als auch (b) die bereits vorab dem Auftragsverarbeiter weitergegebene personenbezogene Daten und (c) weitere über das Endgerät des Nutzenden erhobene Informationen (z. B. IP-Adresse, Browser-Kennung, Sprache) informieren müssen. Es ist zu beachten, dass die Datenschutzhinweise nach Art. 13 DS-GVO nicht nur bei der erstmaligen Erhebung von personenbezogenen Daten zu erteilen sind. Art. 13 Abs. 3 DS-GVO normiert auch Informationspflichten, wenn bereits erhobene personenbezogene Daten für einen anderen Zweck als den der Erhebung verarbeitet werden sollen. Er ist

damit einschlägig, wenn die ursprünglich zu anderen Zwecken erhobenen Stammdaten der Beschäftigten nun zur Durchführung der Mitarbeitendenbefragung verwendet werden.

Die Ergebnisse der Mitarbeitenbefragung waren für das Unternehmen auch nicht anonym. Anonym sind Daten, die sich nicht im Sinne von Art. 4 Nummer 1 DS-GVO auf eine identifizierte oder identifizierbare natürliche Person beziehen. Bei der Prüfung der Identifizierbarkeit einer natürlichen Person sollen nach Erwägungsgrund 16 Satz 3 DS-GVO „alle Mittel" berücksichtigt werden, die von dem Verantwortlichen oder „einer anderen Person nach allgemeinem Ermessen wahrscheinlich" genutzt werden, um die natürliche Person „direkt oder indirekt" zu identifizieren.

Auch nach der Rechtsprechung des EuGH besteht ein Personenbezug für die Personen oder Stellen, die über Mittel verfügen oder Zugang zu Mitteln haben, die nach allgemeinem Ermessen wahrscheinlich für die Identifizierung der von den Daten betroffenen Person genutzt werden (EuGH, Urteil vom 04.09.2025 - C-413/23 P - GRUR-RS 2025, 22620, Rn. 87). Von einer Anonymität kann insbesondere deshalb nicht gesprochen werden, da der die Umfrage durchführende Dienstleister nach Art. 28 Abs. 3 Buchst. a) DS-GVO personenbezogene Daten nach den Weisungen des Unternehmens verarbeitet. Dieses ist datenschutzrechtlich nach Art. 4 Nummer 7 DS-GVO „Verantwortlicher" und eine Weisung, die individuell zu einem Mitarbeitenden gespeicherten personenbezogenen Daten an dieses herauszugeben, muss möglich sein (z. B. bei Geltendmachung eines Betroffenenrechts zur Auskunftserteilung nach Art. 28 Abs. 3 Buchst. e) DS-GVO oder zur Wahrung der Kontrollbefugnisse nach Art. 28 Abs. 3 Buchst. h) DS-GVO).

Art. 5 Abs. 1 Buchst. a) DS-GVO normiert den Grundsatz der Transparenz der Datenverarbeitung und der Verarbeitung nach Treu und Glauben. Mit diesen Grundsätzen ist es nicht vereinbar, wenn ein Verantwortlicher gegenüber betroffenen Personen falsche Angaben über die Verarbeitung ihrer personenbezogenen Daten macht. Hinsichtlich der Inhalte der Transparenz der Datenverarbeitung hält Erwägungsgrund 39 Satz 2 DS-GVO fest, dass „für natürliche Personen Transparenz dahin gehend bestehen [sollte], dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden."

Die Transparenz betrifft nach Erwägungsgrund 39 Satz 4 DS-GVO vor allem die Identität des Verantwortlichen, die verarbeiteten Daten, den Zweck der Datenverarbeitung, die Schritte der Datenverarbeitung, die Empfänger übermittelter Daten, die Quellen der Daten, die Rechtsgrundlage der Datenverarbeitung und „sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden." Verantwortliche tragen dem Grundsatz der Transparenz der Datenverarbeitung insbesondere durch korrekte Informationen der betroffenen Personen nach Art. 13 bzw. 14 DS-GVO Rechnung.

Der Grundsatz der Verarbeitung personenbezogener Daten nach Treu und Glauben ist ein Auffangtatbestand und ihm unterfallen z. B. Verhaltensweisen, die berechtigtes Vertrauen verletzen. Berechtigtes Vertrauen kann explizit über Absprachen oder vorausgegangenes Verhalten hervorgerufen werden oder implizit über berechtigte Erwartungen in die Einhaltung von Verkehrs-, Handels- oder Berufsregeln. Im vorliegenden Fall hat das Unternehmen gegenüber seinen Beschäftigten wiederholt angegeben, dass die Verarbeitung der in der Mitarbeitendenbefragung gegebenen Antworten anonym sei. Da die Antworten der Beschäftigten jedoch personalisiert bei seinem Auftragsverarbeiter vorlagen, konnte auch das Unternehmen auf die Antworten zugreifen, indem es seine Rechte als Verantwortlicher geltend macht. Durch die irreführenden Angaben über die Anonymität der Umfrage wurden die Beschäftigten ggf. verleitet, Angaben zu machen, die sie ansonsten nicht gemacht hätten und von denen sie nicht gewollt hätten, dass ihr Arbeitgeber sie erfährt.

Eine Mitarbeitendenbefragung datenschutzkonform durchzuführen ist eine Herausforderung. Eine Möglichkeit ist es, nur solche Fragen zu stellen, die zur Durchführung des Beschäftigungsverhältnisses erforderlich sind, Dann kann die Befragung auf Art. 6 Abs. 1 Buchst. b) DS-GVO gestützt werden. Alternativ könnte die Teilnahme an der Umfrage freigestellt und nur solche Datenverarbeitungen im Zusammenhang mit ihr vorgenommen werden, in die die Beschäftigten eingewilligt haben. Dann dürfen die Beschäftigten jedoch nicht unter Druck gesetzt werden, an der Umfrage teilzunehmen. Auf jeden Fall müssen die Mitarbeitenden informiert werden, welche personenbezogene Daten von ihnen im Zusammenhang mit der Umfrage verarbeitet werden. Wir haben dem Unternehmen Hinweise erteilt,

wie Mitarbeitendenbefragungen in Zukunft datenschutzkonform durchgeführt werden können. Zudem haben wir aufgrund der festgestellten Verstöße eine Verwarnung nach Art. 58 Abs. 2 Buchst. b) DS-GVO ausgesprochen.

5.5.7. Wie siehts mit der Erforderlichkeit aus?

Art. 57 Abs.1 Buchst. a), f) DS-GVO

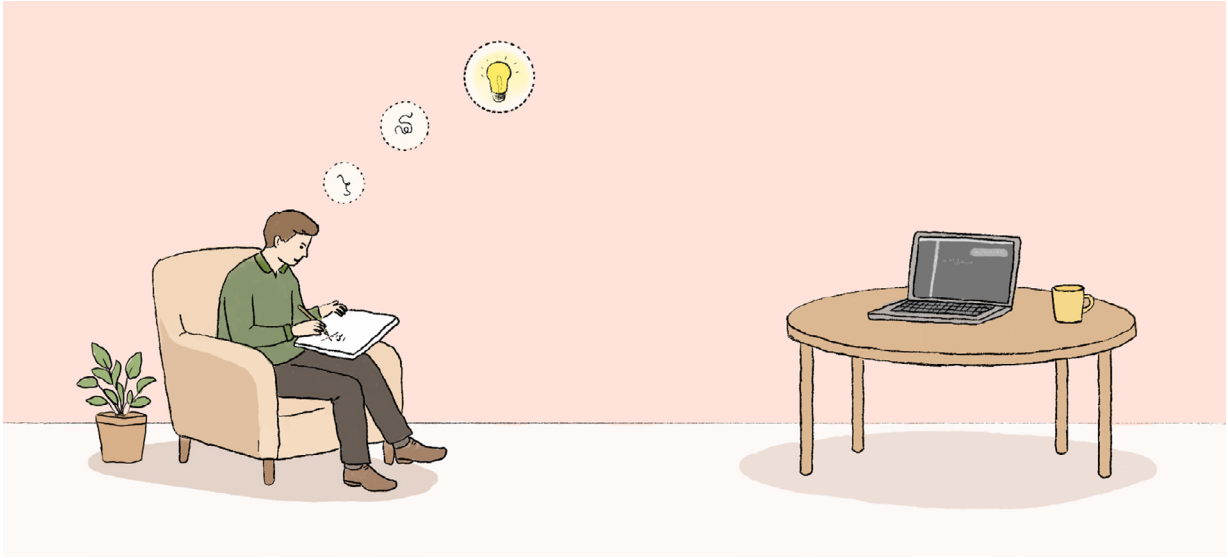
Natürlich benötigt ein Unternehmen Daten von Käufer_innen, um mit diesen einen Vertrag abschließen und diesen erfüllen zu können. Diese Form der Datenerhebung und Datenverarbeitung sieht Art. 6 Abs.1 Satz 1 Buchst. b) DS-GVO auch ausdrücklich vor. Hierbei dürfen vom Verantwortlichen aber nur die für die konkrete Vertragserfüllung erforderlichen Daten verarbeitet werden. In der Praxis wird das Kriterium der Erforderlichkeit aber oft sehr weit – manchmal leider auch zu weit, wie hier im Falle eines Messeveranstalters – ausgelegt.

Ein Messeveranstalter bietet auf seiner Internetseite Eintrittstickets für seine Messe auf dem Stuttgarter Messegelände an. Ein Kunde, der Messetickets online kaufen wollte, beschwerte sich anschließend bei uns darüber, dass neben den üblichen Vertragsdaten (Ticketanzahl, Name, Vorname, Anschrift, E-Mail-Adresse und Zahlungsdaten des Kunden) in der Kaufabwicklung eine Rubrik für ziemlich persönliche Fragen an den Kunden vorgesehen war – und zwar ausgestaltet als Pflichtfelder. Hierbei ging es u.a. um persönliche Vorlieben bzw. Interessen im Hinblick auf das Messethema, um Kaufabsichten, das Alter der Kundschaft u. ä.

Ohne die Beantwortung dieser Fragen konnte man im Rahmen der Kaufabwicklung nicht den nächsten Reiter der Internetseite aufrufen und folglich den Ticketkauf nicht abschließen.

Im Beschwerdeverfahren hat sich der Vorwurf des Petenten bestätigt. Daher haben wir das Unternehmen darauf hingewiesen, dass im Rahmen des Art. 6 Abs.1 Satz 1 Buchst. b) DS-GVO nur jene Daten erhoben und verarbeitet werden dürfen, die konkret für die Vertragserfüllung und Vertragsabwicklung mit dem Kunden erforderlich sind. Die Verarbeitung ist jedenfalls erforderlich, wenn der Vertrag ohne Verarbeitung der Daten in dem geltend gemachten Umfang nicht erfüllt werden könnte. Die Erhebung von Antworten auf persönliche Fragen über Vorlieben und Interessen gehören im Hinblick auf einen Ticketverkauf sicherlich nicht dazu, da kein unmittelbarer Zusammenhang zwischen der Verarbeitung dieser Daten und dem konkreten Zweck des Vertragsverhältnisses besteht.

Wir forderten das Unternehmen daher auf, diesen Fragenkatalog aus dem Kaufprozess zu entfernen und



Fabrizio Matarese / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

sämtliche Daten, die bislang aus den Fragestellungen erhoben wurden, dauerhaft zu löschen. Das Unternehmen kam dieser Aufforderung umgehend nach.

In zahlreichen Beratungsanfragen und Beschwerdeverfahren wird diese Thematik an uns herangetragen, da immer wieder zwischen den Kund_innen und den verantwortlichen Stellen unterschiedliche Meinungen vorherrschen, welche Daten zur Vertragserfüllung erforderlich sind und welche nicht. In mehreren Entscheidungen hat sich auch der Europäische Gerichtshof mit dieser Fragestellung befasst und dabei inzwischen strenge Regeln im Hinblick auf die Erforderlichkeit aufgestellt:

Zunächst hat der EuGH mehrfach betont, dass die in Art. 6 Abs.1 Satz 1 Buchst. b) bis f) DS-GVO vorgesehenen Rechtfertigungsgründe eng auszulegen sind, da sie dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist (u.a. Urteil vom 4. Juli 2023, Meta Platforms u.a. [Allgemeine Nutzungsbedingungen eines sozialen Netzwerks], C-252/21, EU:C:2023:537, Rn. 93; Urteil vom 12. September 2024, HTB Neunte Immobilien Portfolio und Ökorenta Neue Energien Ökostabil IV, C-17/22 und C-18/22, EU:C:2024:738, Rn. 37).

Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich angesehen werden kann, müsse sie objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Der Verantwortliche müsse nachweisen können, inwiefern der Hauptgegenstand des Vertrags ohne die betreffende Verarbeitung nicht erfüllt werden könne (a.a.O., Rn. 98). Entscheidend für die Anwendung des in Art. 6 Abs.1 Satz 1 Buchst. b) DS-GVO genannten Rechtfertigungsgrundes sei somit, dass die Verarbeitung personenbezogener Daten durch den Verantwortlichen für die ordnungsgemäße Erfüllung des zwischen ihm und der betroffenen Person geschlossenen Vertrags wesentlich ist und dass daher keine praktikablen und weniger einschneidenden Alternativen bestehen (Urteil vom 4. Juli 2023, Meta Platforms, Rn. 99). Der Gerichtshof hat zudem entschieden, dass nach Art. 5 DS-GVO der Verantwortliche die Beweislast dafür trägt, dass die Daten u.a. für festgelegte, eindeutige und legitime Zwecke erhoben und auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Noch strengere Maßstäbe legte der EuGH schließlich in seinem Urteil vom 9. Januar 2025 (C-394/23) an, bei dem es um die Erhebung der Anrede der Kundschaft beim Onlinekauf eines Bahntickets bei der französischen SNCF ging: Damit eine Verarbeitung personenbezogener Daten als für die Erfüllung eines Vertrags erforderlich im Sinne dieser Bestimmung angesehen werden könne, müsse sie – entsprechend der Meta-Entscheidung – objektiv unerlässlich sein, um einen Zweck zu verwirklichen, der notwendiger Bestandteil der für die betroffene Person bestimmten Vertragsleistung ist. Eine solche Kommunikation müsse jedoch nicht notwendigerweise anhand der Geschlechtsidentität des betreffenden Kunden personalisiert werden. Nach der Rechtsprechung des EuGH erscheint die Personalisierung von Inhalten nämlich nicht erforderlich, um einem Kunden Dienste anzubieten, wenn diese Dienste gegebenenfalls in Form einer gleichwertigen Alternative an ihn erbracht werden können, die nicht mit einer solchen Personalisierung verbunden ist, so dass diese nicht objektiv unerlässlich ist, um einen Zweck zu verwirklichen, der notwendiger Bestandteil dieser Dienste ist.

Und der EuGH fährt fort: „Was die im Ausgangsverfahren in Rede stehenden Dienstleistungen betrifft, erscheint eine Personalisierung der geschäftlichen Kommunikation, die auf einer anhand der Anrede angenommenen Geschlechtsidentität beruht, weder objektiv unerlässlich noch wesentlich, um die ordnungsgemäße Erfüllung des betreffenden Vertrags im Sinne der in den Rn. 33 und 34 des vorliegenden Urteils angeführten Rechtsprechung zu ermöglichen“ (a.a.O., Rn. 39).

Für die Bewertung der Erforderlichkeit spielt nach Auffassung des EuGH die Verkehrssitte oder Gepflogen-

Infokasten

Im Kontext von digitalen Dienstleistungen hat der Europäische Datenschutzausschuss (EDSA) Leitlinien zur Auslegung des Merkmals der Erforderlichkeit zur Vertragserfüllung entwickelt, die hier veröffentlicht sind: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_de

heit (Höflichkeit, Umgangsformen) grundsätzlich keine Rolle. Welche Daten für die konkrete Vertragsdurchführung erforderlich sind, ist nach der aktuellen Rechtsprechung des EuGH eng auszulegen: Nur die Daten, die objektiv für die Vertragserfüllung unverzichtbar sind, dürfen verarbeitet werden.

Die verantwortlichen Stellen sollten daher auch wegen des Grundsatzes der Datenminimierung, der in Art. 5 Abs.1 Buchst. c) DS-GVO verankert ist und verlangt, dass personenbezogene Daten „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt" sind, sorgfältig prüfen und dokumentieren, warum sie welche Daten für welche konkreten Zwecke bei der Vertragserfüllung verarbeiten.

5.5.8. Verwarnung eines politischen Vereins

Art. 57 Abs.1 Buchst. a) DS-GVO

Verantwortliche haben bei Betrieb von Webseiten und Newslettern wirksame Maßnahmen zum Schutz personenbezogener Daten zu treffen. Dies gilt auch – und gerade – für politische Vereine, da Rückschlüsse auf politische Positionen der Mitglieder und Unterstützer möglich sind und mithin ein erhöhtes Risiko für die Rechte und Freiheiten betroffener Personen besteht.

Auf der Webseite eines politischen Vereins war Interessenten die Möglichkeit eröffnet worden, Spenden an den Verein zu geben und Newsletter des Vereins zu abonnieren. Wegen nicht ausreichender Schutzmaßnahmen zur Sicherung von Schlüsselmaterial und Schnittstelle auf dem Webserver kam es 2024 zu mehreren zusammenhängenden Datenpannen, bei der insb. Name und E-Mailadresse und die Zugehörigkeit zu Mailing-Listen „Spender unter 500 Euro" und „Spender über 500 Euro" betroffen waren. Der oder die Angreifer konnten hierbei Schlüsselmaterial zur Schnittstelle des Newsletter-Dienstleisters vom Webserver des Vereins auslesen und damit personenbezogene Daten bei dem Newsletter-Dienstleister des Vereins abrufen und löschen.

Wir haben gegen den Verein wegen mangelnden Schutzes der Vertraulichkeit und Integrität eine Verwarnung ausgesprochen. Hierbei standen primär im Fokus unserer Entscheidung unzureichende Maßnahmen im Vorfeld der Datenpanne, welche diese ermöglicht bzw. begünstigt haben. Allgemein empfehlen wir – neben dem Verweis auf die exemplarisch unten verlinkten Hinweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) – insbesondere folgende Schutzmaßnahmen:

- Deaktivierung des sog. „Directory Listing" beim Webserver
- Speicherung nur benötigter Dateien auf dem Webserver und möglichst außerhalb des sog. „DocumentRoot" Verzeichnisses (das vom Webserver mittels http veröffentlichte Wurzelverzeichnis)
- Ablagen zur versionierten Speicherung (z. B. git) nicht im „DocumentRoot" und Sicherstellung, dass kein Schlüsselmaterial darin gespeichert wird (auch nicht versehentlich bzw. trotz vermeintlicher Löschung)
- Protokollierung von Zugriffen auf Schnittstellen, insbesondere Fehlzugriffe, aber auch gehäufte Abrufe. Regelmäßige bzw. automatische Auswertung der Protokolle (Log-Monitoring) z. B. von Auffälligkeiten wie Zugriffe von wechselnden IP-Adressen, Abruf großer Mengen und ggf. Sperre (z. B. Rate-Limiting)
- Vergabe minimaler Rechte bei Schnittstellen („Least Privileges" bzw. Prinzip der geringsten Berechtigungen)

Verantwortliche haben sicherzustellen, dass Schlüsselmaterial für den Zugriff auf API-Zugänge geschützt ist und wirksame Maßnahmen zum Schutz der Verarbeitung an der technischen Schnittstelle getroffen sind.

Infokasten

Weiterführende Links:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Webanwendungen/Webanw_Auftragnehmer.pdf

BSI-Kompendium, insb. APP.3.2 Webserver:
https://bsi.bund.de/kompendium/

5.5.9. Veröffentlichung von Wahlergebnissen im Internet

Art. 57 Abs.1 Buchst. a) DS-GVO

Im Jahr 2025 erreichte uns eine "Datenpannenmeldung" (s. Art. 33 DS-GVO), wonach unter anderem Wahlergebnisse zu einer Wahl der Jugend- und Auszubildendenvertretung, einer Wahl zur Mitarbeitendenvertretung und einer Wahl zur Schwerbehindertenvertretung im Internet abrufbar waren. Dies war sogar noch Ende Januar 2025 der Fall, obwohl die Wahlen bereits 2024 stattgefunden hatten. Die Wahlergebnisse konnten auch über Suchmaschinen gefunden werden.

Die Dateien enthielten insbesondere den Namen der Personen, die auf den genannten Listen standen, und deren Stimmenanzahl und Listenplatzierung. Bei dem Wahlergebnis zur Schwerbehindertenvertretung wurden auch die Geburtsdaten der gewählten Vertrauensperson sowie der gewählten Stellvertretungen genannt. Ursache für die Veröffentlichung im Internet war wohl, dass diese Inhalte bei einer Migration der Inter- und Intranetseiten des Verantwortlichen aus Versehen auf eine öffentlich zugängliche Website umgezogen worden waren.

Die Ergebnisse von Wahlen zur Jugend- und Auszubildendenvertretung, zur Mitarbeitendenvertretung und zur Schwerbehindertenvertretung sind nach den einschlägigen Vorschriften innerhalb des Betriebs bzw. der Dienststelle, bei der die Wahl stattgefunden hat, den Wahlberechtigten für zwei Wochen bekanntzumachen. Dies ergibt sich für die Wahl zur Mitarbeitendenvertretung aus § 3 Abs. 4 und § 18 der Wahlordnung zum Betriebsverfassungsgesetz (WO) für den Betriebsrat und aus § 2 Abs. 2 und 31 der Wahlordnung zum Landespersonalvertretungsgesetz (LPVGWO) für den Personalrat. Für die Wahl zur Jugend- und Auszubildendenvertretung gelten die genannten Vorschriften nach § 39 Abs. 2 Satz 2 WO bwz. § 54 Abs.1 LPVGWO entsprechend. Die Veröffentlichung des Ergebnisses der Wahl zur Schwerbehindertenvertretung regeln § 5 Abs. 2 und § 15 Wahlordnung Schwerbehindertenvertretungen (SchwbVWO).

Die genannten Vorschriften liefern somit eine Grundlage die personenbezogenen Daten in den genannten Listen für den Zeitraum intern zu veröffentlichen. Nach Art. 6 Abs.1 Buchst. c) DS-GVO sind Verarbeitungen personenbezogener Daten zulässig, wenn sie zur Erfüllung einer rechtlichen Pflicht erforderlich sind. Eine solche Pflicht ist auch die Veröffentlichung der Wahlergebnisse in dem von den gennannten Vorschriften vorgesehenen Umfang. Ob die Veröffentlichung durch Aushang oder auf elektronischem Weg, etwa im Intranet, erfolgt, ist nicht relevant. Es gibt allerdings keine Grundlage dafür, die Wahlergebnisse Personen zugänglich zu machen, die nicht Teil der wählenden Stelle sind, oder diese länger als zwei Wochen zu veröffentlichen.

Eigentlich sollten die Wahlergebnisse nur im Intranet der verantwortlichen Stelle veröffentlicht und auch nur befugten Personen nach einem Log-in mit ID und Passwort zugänglich sein.

Nach weiteren Ermittlungen zu der Datenpanne fiel uns zudem auf, dass die Wahlergebnisse trotz Löschung von der eigentlichen Internetseite noch weiterhin über die Internet Wayback Machine abrufbar waren (s. https://web.archive.org/). Daher traten wir an die meldende Stelle heran und forderten sie auf, einen Löschantrag zu stellen (s. How do I request to remove something from archive.org? – Internet Archive Help Center: https://help.archive.org/help/how-do-i-request-to-remove-something-from-archive-org/).

Ermittlungen zur Ursache der Datenpanne und das angeforderte Migrationsprotokoll ergaben, dass wohl nicht sorgfältig genug geprüft worden war, ob Zugriffsbeschränkungen übernommen worden waren. Die Person, welche die Migration durchgeführt hat, war bei dieser im internen Netz des Verantwortlichen eingeloggt. Sie hat wohl nicht gesehen, dass die Inhalte zugriffsbeschränkt waren. Nach einem Migrationsprozess, bei dem zugriffsbeschränkte Inhalte mit personenbezogenen Daten migriert werden, muss eine Kontrolle spezifisch darauf, ob die Zugriffsberechtigungen korrekt übernommen werden, durchgeführt werden. Nach der Migration müssen zudem Tests durch die IT-Abteilung und eine Endkontrolle durch die für die Inhalte verantwortliche Einheit durchgeführt werden. Zudem muss der migrierenden Person bewusst sein, welche Inhalte zugriffsbeschränkt sind. Dies muss entweder in einem Migrationsplan aufgeführt werden oder in den Metadaten der zu migrierenden Webseite angegeben sein.

Weiter war für uns relevant, dass die Wahlergebnisse deutlich länger als die vorgesehenen zwei Wochen veröffentlicht wurden. Die verantwortliche Stelle

erklärte im Laufe des Verfahrens, die rechtzeitige Löschung von Inhalten auf ihren Inter- und Intranetseiten durch systemseitige Erinnerungs- bzw. Kennzeichnungsfunktionen bzw. durch Anpassungen im Redaktions-Workflow sicherzustellen. Dies ist zumindest dann als ausreichende Maßnahme anzusehen, wenn keine Möglichkeit besteht, eine automatisierte Löschung der Inhalte nach der vorgegebenen Dauer zu erreichen, ohne dass dies zu einer Beeinträchtigung der Sicherheit bzw. Funktionsfähigkeit der Webseite führen würde.

Im Laufe des Verfahrens überarbeitete die verantwortliche Stelle das Migrationskonzept und ergänzte es um Regelungen zum Umgang mit zugriffsbeschränkten Inhalten. Weiterhin stellte sie einen Löschantrag, worauf die beanstandeten Inhalte auch aus dem Archiv der Internet Wayback Machine gelöscht wurden.

Aus diesem Verfahren lassen sich für Verantwortliche gleich mehrere Lehren ziehen: Bei einer Migration von Webseiten ist sorgfältig darauf zu achten und zu kontrollieren, ob Zugriffsbeschränkungen auf personenbezogene Inhalte übernommen wurden. Zudem ist durch angemessene technische und organisatorische Maßnahmen sicherzustellen, dass personenbezogene Daten, die nur eine bestimmte Zeit lang veröffentlicht werden sollen, nach Ablauf dieser Zeit auch tatsächlich wieder gelöscht werden. Hierbei stellen sich besondere Herausforderungen bei dem Entfernen von Inhalten aus dem Internet, sofern diese von Suchmaschinen indiziert oder in das Archiv der Internet Wayback Machine aufgenommen worden sind.

5.5.10. Internationaler Datentransfer: Das Gericht der Europäischen Union hat gesprochen. Eine Einordnung

Art. 57 Abs.1 Buchst. i) DS-GVO

Der Datentransfer zwischen Deutschland und den USA ist – aufgrund der engen wirtschaftlichen Beziehungen – von großer praktischer Bedeutung und häufig Gegenstand von Anfragen. Deshalb berichten wir regelmäßig über aktuelle Entwicklungen (zuletzt im 36. Tätigkeitsbericht Datenschutz 2020, S. 47 ff. und im 39. Tätigkeitsbericht Datenschutz 2023, S. 103 f.). Wie dort ausgeführt, hat der Angemessenheitsbeschluss zwar vorläufige Rechtssicherheit geschaffen. Wie prophezeit, war damit aber nicht das letzte Wort in Sachen Datenübermittlungen in die USA gesprochen. So hatte der EU-Parlamentsabgeordnete Philippe Latombe zwischenzeitlich Klage gegen den Angemessenheitsbeschluss eingereicht. Der Ausgang des Verfahrens war auf Grund seiner Bedeutung für die unternehmerische und aufsichtsbehördliche Praxis mit Spannung erwartet worden.

Am 3. September 2025 hat das Gericht der Europäischen Union (EuG) die von dem französischen Abgeordneten Philippe Latombe erhobene Nichtigkeitsklage gegen den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US Data Privacy Framework (DPF) abgewiesen.

Damit wurde erstmals die Gültigkeit eines US-Angemessenheitsbeschlusses gem. Art. 45 Abs.1 DS-GVO nicht nur inzident im Rahmen eines Vorabentscheidungsverfahrens, sondern unmittelbar in einem Nichtigkeitsverfahren überprüft und erstinstanzlich bestätigt.

Der Kläger hatte im Wesentlichen geltend gemacht, der DPF verstoße gegen Art. 7, 8 und 47 der Charta der Grundrechte der Europäischen Union (GRCh). Zentrale Angriffspunkte waren die weiterhin mögliche „bulk collection“ durch US-Nachrichtendienste ohne unabhängige Vorabkontrolle sowie die fehlende Unabhängigkeit und Gerichtseigenschaft des neu geschaffenen Data Protection Review Court (DPRC). Ergänzend rügte der Kläger Verstöße gegen Art. 22 und Art. 32 DS-GVO.

Das EuG hat die Frage der Zulässigkeit der Klage ausdrücklich offengelassen. Obwohl erhebliche Zweifel an der individuellen Betroffenheit des Klägers bestanden, hat das Gericht – im Interesse einer geordneten Rechtspflege – unmittelbar die Begründetheit geprüft. Diese Vorgehensweise ist ungewöhnlich und unterstreicht die grundsätzliche Bedeutung der Sache.

Für die rechtliche Bewertung stellt das EuG entscheidend darauf ab, dass die Rechtmäßigkeit eines Unionsrechtsakts in einem Nichtigkeitsverfahren gem. Art. 263 Abs. 4 AEUV ausschließlich nach der Sach- und Rechtslage zum Zeitpunkt seines Erlasses zu beurteilen ist. Maßgeblich war daher allein der Stand im Juli 2023, also der Zeitpunkt des Erlasses des Angemessenheitsbeschlusses. Spätere politische oder rechtliche Entwicklungen dürfen nach ständiger Rechtsprechung

nicht berücksichtigt werden. Der Grund hierfür liegt darin, dass die Kommission nur für die damalige Lage Verantwortung trägt und die Rechtmäßigkeit eines Rechtsakts nicht von nachträglichen Veränderungen abhängig gemacht werden darf.

Gerade dieser Punkt schränkt die Aussagekraft des Urteils erheblich ein. Denn die seit Anfang 2025 erfolgten Amtsenthebungen mehrerer Mitglieder unabhängiger US-Aufsichtsorgane, insbesondere bei der Federal Trade Commission (FTC) sowie beim Privacy and Civil Liberties Oversight Board (PCLOB), konnten vom Gericht nicht einbezogen werden. Diese Entlassungen erfolgten erst lange nach Erlass des Angemessenheitsbeschlusses und lagen damit außerhalb des entscheidungserheblichen Zeitraums.

Das EuG weist in diesem Zusammenhang ausdrücklich auf die Pflicht der Kommission hin, den Beschluss fortlaufend zu überwachen und bei relevanten Entwicklungen gegebenenfalls zu ändern, auszusetzen oder zu widerrufen. Die Verantwortung für den Umgang mit solchen späteren Entwicklungen wird somit von der gerichtlichen Kontrolle auf die politische und administrative Ebene der Kommission verlagert.

In der Sache selbst sieht das EuG keinen Verstoß gegen Art. 47 GRCh. Das DPRC sei trotz seiner besonderen Einbettung in die US-Exekutive hinreichend unabhängig. Maßgeblich seien die Regelungen zur Ernennung und Abberufung der Richter, die im Wesentlichen mit denen der US-Bundesrichterschaft vergleichbar seien. Die vom EuGH in Schrems II beanstandeten Mängel der Ombudsperson – fehlende Unabhängigkeit und fehlende Entscheidungsbefugnis – würden dadurch behoben. Auch die Frage, ob es sich um ein „durch Gesetz errichtetes Gericht“ handelt, beantwortet das EuG funktional und nicht formal: Entscheidend seien Befugnisse, Verfahrensgarantien und tatsächliche Unabhängigkeit, nicht formelle Gesichtspunkte wie die äußere institutionelle Einordnung.

Hinsichtlich der Art. 7 und 8 GRCh gelangt das Gericht zu dem Ergebnis, dass die fehlende unabhängige Vorabkontrolle bei „bulk collection“ keinen Verstoß begründet. Das EuG betont, dass weder aus Schrems II noch aus der Rechtsprechung des EGMR zwingend eine vorgelagerte Genehmigungspflicht folge. Zwar erkennt das Gericht die Relevanz der EGMR-Entscheidung „Big Brother Watch“ an, legt deren Anforderungen jedoch im Lichte des Maßstabs der Angemessenheitsprüfung aus: Drittstaaten müssten kein identisches, sondern lediglich ein im Wesentlichen gleichwertiges Schutzniveau gewährleisten.

Problematisch ist aus aufsichtsrechtlicher Sicht insbesondere, dass das EuG die „bulk collection“ als ersten Schritt eines mehrstufigen Verarbeitungsprozesses betrachtet und geringere Schutzanforderungen für die anfängliche Datenerhebung genügen lässt. Diese Sichtweise steht in Spannung zur Rechtsprechung des EGMR, der eine Gesamtbetrachtung aller Verarbeitungsphasen fordert, sowie zur Stellungnahme 5/2023 des EDSA, die sowohl eine unabhängige Vorabkontrolle als auch eine systematische Ex-post-Kontrolle angemahnt hatte. Mit dieser differenzierten Kritik setzt sich das EuG nicht vertieft auseinander, sondern verweist darauf, dass der EDSA-Stellungnahme keine verbindliche Rechtswirkung zukomme.

Vor diesem Hintergrund bleibt festzuhalten, dass das Urteil zwar die Angemessenheitsentscheidung formal bestätigt, die materiellen Zweifel an der tatsächlichen Wirksamkeit der US-Schutzmechanismen jedoch nicht vollständig ausräumt. Die Eingriffe in die personelle Unabhängigkeit von FTC und PCLOB durch politisch motivierte Entlassungen einzelner Mitglieder verstärken diese Zweifel, konnten aber aufgrund des maßgeblichen Entscheidungszeitpunkts zumindest in diesem Verfahren (noch) keine Rolle spielen. Sie gewinnen jedoch erhebliche Bedeutung für die laufende Überwachungspflicht der Kommission und für eine mögliche Überprüfung durch den Europäischen Gerichtshof in möglichen Vorabentscheidungsverfahren.

Kurz- und wohl auch mittelfristig bleibt somit der DPF anwendbar. Das Urteil schafft jedoch keine endgültige Rechtssicherheit. Der Kläger hat am 31. Oktober 2025 Berufung beim Europäischen Gerichtshof gegen das erstinstanzliche Urteil des Gerichts der Europäischen Union eingereicht (C-703/25 P); zudem sind weitere Gerichtsverfahren möglich. Langfristig wird entscheidend sein, ob der EuGH bei einer erneuten Prüfung stärker auf die tatsächliche Funktionsfähigkeit und politische Stabilität der US-Aufsichts- und Rechtsschutzmechanismen abstellt. Die jüngsten Entwicklungen bei FTC und PCLOB könnten dabei ein größeres Gewicht erlangen als es in diesem Verfahren vor dem EuG der Fall war.

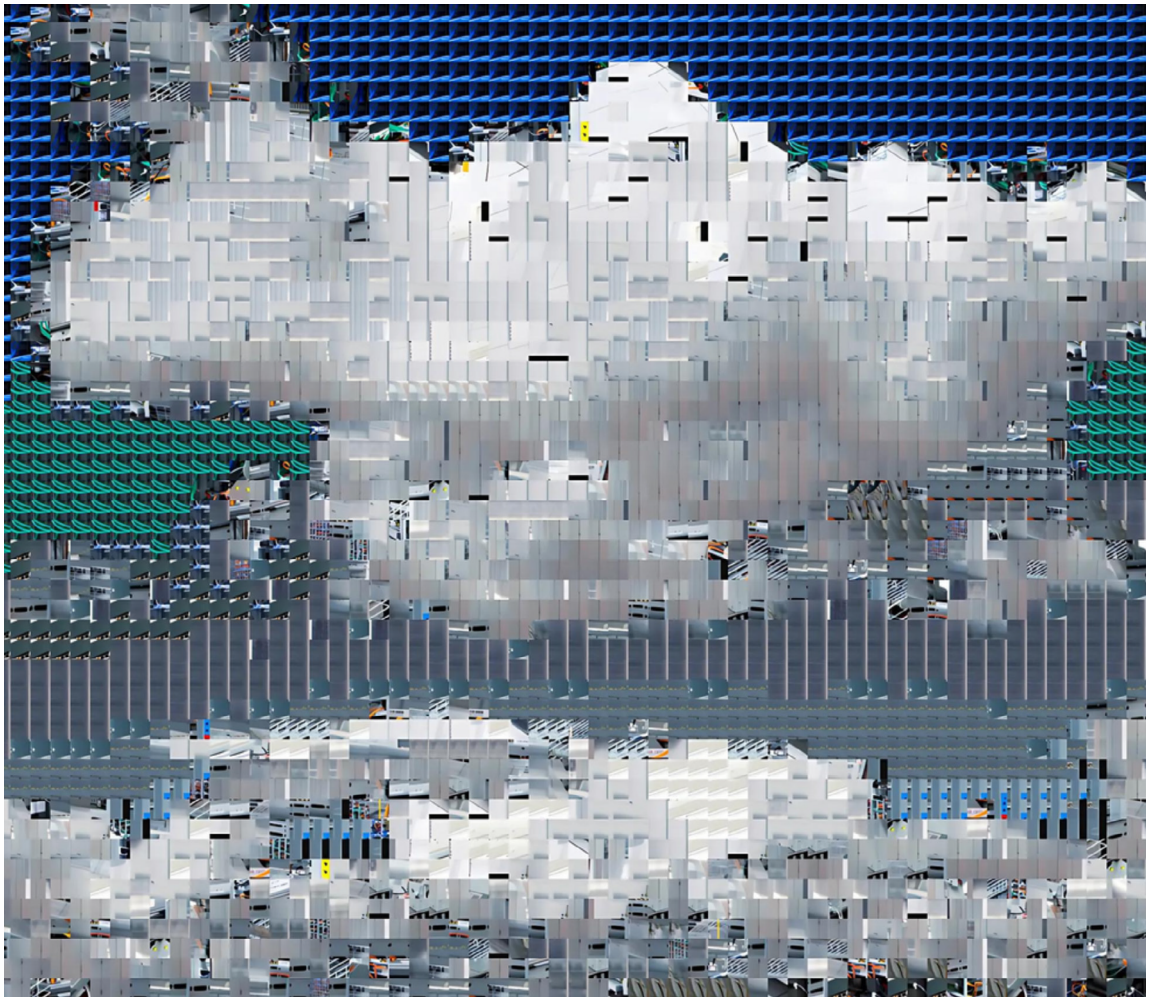


Bild: Nadia Piet & Archival Images of AI + AIxDESIGN / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

5.6. Abteilung 5: Technisch-organisatorischer Datenschutz, Datensicherheit

Unsere Fachleute aus dieser Abteilung haben klar die technische Seite des Datenschutzes im Blick. Sie haben ein eigenes Prüflabor und befassen sich rechtlich und technisch mit sogenannten TOM, also den technischen und organisatorischen Maßnahmen von verantwortlichen Stellen wie Behörden und Unternehmen.

5.6.1. Identitätsfeststellung durch Fingerabdruckabgleich per App

§ 98 Abs.1 Nr. 3 Polizeigesetz

Im Zuge einer Beratung zum Einsatz einer App der Polizei Baden-Württemberg haben wir uns mit Datensicherheit und der Aussagekraft von Analysen und Bewertungen beschäftigt. Im konkreten Fall konnten alle ursprünglichen Anlässe für Bedenken aufgeklärt oder ausgeräumt werden. Weil uns bei der Einführung und Entwicklung von Apps und anderer Software einige Fragen immer wieder begegnen, haben wir diese in diesem Beitrag kurz zusammengefasst.

Zum konkreten Beratungsverfahren: Um die Personalien von Personen ohne Ausweisdokumente unterwegs feststellen zu können, führt die Polizei Baden-Württemberg die App mDakty auf ihren dienstlichen Smartphones ein. Wie in mehreren anderen Bundesländern können Polizeikräfte mit dieser die Fingerabdrücke von Betroffenen aufnehmen und mit Polizeidatenbanken abgleichen, ohne dafür auf die nächste Wache fahren zu müssen. Sind die Fingerabdrücke der betroffenen Person in einer Polizeidatenbank enthalten, beispielsweise weil den Betroffenen zuvor in einem Ermittlungsverfahren mittels ED-Behandlung die Fingerabdrücke genommen und gespeichert wurden, wird in der App ein Treffer mit einer ID angezeigt. Mit letzterer können die Polizeikräfte die zu der Person gespeicherten Daten (beispielsweise Name, Adresse und Foto) über die App mARS, die bereits in Verwendung ist, abfragen.

Die Polizei darf auf Grundlage verschiedener gesetzlicher Regelungen Fingerabdrücke erheben und abgleichen, z. B. zum Zwecke der Identitätsfeststellung nach §§ 41, 47 Polizeigesetz (PolG). Dies ist bereits jetzt möglich, durch mDakty und mARS kann es allerdings mobil erfolgen: Durch die Gestaltung als App auf den dienstlichen Smartphones entfällt die Anreise zu einer Wache, um die dortige Technik zu nutzen. In unserer Beratung zu mDakty ging es dementsprechend im Wesentlichen darum, ob die technische Umsetzung des Erhebens und Abgleichens von Fingerabdrücken in den genannten Apps datenschutzkonform und sicher gestaltet ist.

Teil der von uns angeforderten technischen Unterlagen war ein Bericht einer statischen Code-Analyse der App. In diesem wurden mehrere deaktivierte Sicherheitsfeatures sowie URLs von externen Diensten genannt. In einem produktiven Austausch mit der Polizei sowie dem IT-Dienstleister, welcher für die Erstellung der App zuständig ist, konnten Bedenken ausgeräumt und Anpassungen durchgeführt werden. Insbesondere stellte sich heraus, dass die URLs nicht aktiv waren bzw. nur in der Dokumentation auftauchten und die Kommunikation mit Drittdiensten ohnehin blockiert ist. Auch eine auf unsere Hinweise durchgeführte Netzwerkverbindungsanalyse ergab keine Verbindungsversuche nach Außen.

Im Zuge unserer Beratung wurde außerdem die Testumgebung angepasst. Dadurch konnten Sicherheitsausnahmen in der App entfernt und damit potentielle Risiken weiter reduziert werden. Die wiederkehrenden Themen bei Einführung und Entwicklung von Apps und anderer Software, die grundsätzlich beachtet werden sollten:

Ergebnisse von Prüfungen bedürfen einer Bewertung

Besonders bei einem negativen, regelmäßig jedoch auch bei einem positiven Prüfergebnis, bedarf ein Bericht von (automatisierten) Prüfwerkzeugen einer zusätzlichen Bewertung. Diese muss die entsprechenden falsch-positiven Befunde begründet entkräften. Nur mit einer solchen Bewertung und Einordnung der Befunde kann ein (automatisiert erstellter) Bericht einem prüfbaren Nachweis dienen. Entsprechend sollte eine solche Bewertung zumindest bei negativen Befunden im Prüfbericht zu den üblichen Schritten vor dem Ausrollen neuer App-Versionen gehören. Unabhängig davon, ob die Prüfungen intern oder extern durchgeführt werden, ist es essentiell, dass die Kompetenz zur Durchführung solcher Bewertungen intern vorhanden ist.

Kommunikation ausschließlich zu klar spezifizierten Endpunkten

Zur Verhinderung von Datenabflüssen, die z. B. ungewollt aus dem Einsatz von Software Development Kits (SDK) oder sonstiger Bibliotheken resultieren können, sollte überprüft werden, zu welchen Endpunkten Verbindungen aufgebaut werden. Eine solche Prüfung sollten sowohl Entwickler vor Veröffentlichung neuer Versionen durchführen, als auch nutzende Institutionen, vor der Einführung neuer Software sowie regelmäßig nach Updates. Die erwarteten Endpunkte sollten vor Durchführung der Analyse spezifiziert werden, um Abweichungen erkennen zu können.

Für ein möglichst realistisches Prüfergebnis ist die Durchführung von dynamischen Analysen nötig, die den produktiven Einsatzbedingungen so nah wie möglich entsprechen (vgl. auch nächster Punkt).

Statischer Analyse: Beschränkte Aussagekraft

Insbesondere in Bezug auf Netzwerkverbindungen, wie im vorigen Punkt beschrieben, ist die Aussagekraft von statischen Analysen begrenzt, da diese meist lediglich darauf beruhen im Quellcode nach Zeichenketten zu suchen, die URLs sind oder diesen ähneln. Dies kann zu falsch-positiven Ergebnissen führen, wenn beispielsweise in Kommentaren innerhalb des Quellcodes auf bestimmte Internetressourcen verwiesen wird.

Bestenfalls werden falsch-positive Ergebnisse aus statischen Analysen anhand der Ergebnisse dynamischer Analysen widerlegt. Wo dies nicht möglich ist, bedarf es einer nachvollziehbaren und bestenfalls mit Belegen (wie z. B. Screenshots der durchgeführten Prüfungen) unterfütterten Begründung für das Nichtzutreffen der entsprechenden Befunde.

Keine Sicherheitsausnahmen für Testumgebungen in Produktivversionen

Wenn für Entwicklungs- oder Testzwecke Ausnahmen von Sicherheitsfunktionen der Plattformen notwendig sind, sollten diese auf die erfordernden Versionen beschränkt werden und dürfen nicht in den Produktivversionen vorkommen. Aufgrund vielfältiger Mechanismen zum automatisierten Erzeugen spezifischer Versionen für unterschiedliche Umgebungen entspräche dies nicht dem Stand der Technik.

Wenn beispielsweise Sicherheitsmaßnahmen der Transportverschlüsselung für bestimmte Endpunkte deaktiviert werden, um lokale Entwicklung und Tests zu ermöglichen, so stellt dies ein Sicherheitsrisiko dar, wenn diese auch in die Produktivversionen übernommen werden. Wenngleich nicht immer möglich, ist die bessere Lösung, noch die entsprechenden Umgebungen zu gestalten, so dass auch in diesen auf Sicherheitsausnahmen verzichtet werden kann.

5.6.2. „Willkommen in Berlin“ – wenn regionale App-Hinweise zu Datenschutzbeschwerden führen

Art. 57 Abs.1 Buchst. a), f) DS-GVO

Im Jahr 2025 erreichte uns eine Beschwerde zu einer ortsbezogenen Push-Mitteilung einer gängigen Mobilitäts-App zur Bestellung von Fahrdiensten. Der Betroffene schilderte, nach der Landung in Berlin bei eingeschaltetem iPhone, jedoch ohne die App zu öffnen, eine Begrüßung mit dem Text „Willkommen in Berlin“ erhalten zu haben. Nach seiner Auffassung durfte eine solche Meldung nicht erscheinen, da die App in den iOS-Einstellungen nur die Berechtigung besitzt, den Standort „Während der Nutzung“ zu verwenden. Er ging daher davon aus, dass die App seinen Standort unerlaubt im Hintergrund ermittelt habe.

Zur Begründung führte der Beschwerdeführer an, der App-Betreiber verarbeite damit Standortinformationen unter Verstoß gegen die DS-GVO und das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) sowie entgegen der eigenen Datenschutzerklärung. Die Beobachtung, dass die App eine ortsbezogene Meldung ausgab, obwohl sie nicht aktiv genutzt wurde, bewertete der Betroffene als Beleg für ein heimliches Standort-Tracking und somit als unzulässige Datenverarbeitung.

Technische Einordnung

Entscheidend ist die Unterscheidung zwischen der präzisen Standortbestimmung über den iOS-Ortungsdienst (GPS, WLAN oder Mobilfunk) und einer ungefähren Ortszuordnung, die auch ohne Zugriff auf diese Ortungsfunktionen möglich ist. Eine solche grobe Einordnung kann beispielsweise anhand der IP-Adresse der Internetverbindung oder früher gespeicherter Ortsangaben (etwa der zuletzt genutzten Stadt) erfolgen.

Die iOS-Einstellung „Während der Nutzung“ reglementiert den Zugriff auf die präzisen Standortdaten des Geräts, die aus GPS-, WLAN- oder Mobilfunkdaten gewonnen werden. Sie schließt jedoch nicht aus, dass der Anbieter auf Grundlage anderer Hinweise – etwa der Internetverbindung bzw. IP-Adresse – die ungefähre Region erkennt und entsprechende Mitteilungen anzeigt.

Analyse der App-Funktion

Aus technischer Sicht lässt sich eine solche Funktion nachvollziehbar erklären: Viele Dienste zeigen allgemeine Hinweise an, die sich nach Region, Zeitzone oder Sprache richten. Eine App kann beispielsweise „Willkommen in Berlin“ anzeigen, wenn ein Konto zuletzt in Deutschland genutzt wurde oder wenn die IP-Adresse auf eine Verbindung aus dem Berliner Raum schließen lässt. Dabei werden keine neuen, präzisen Standortdaten vom Gerät abgefragt. Die Meldung entsteht vielmehr durch eine serverseitige Logik, die auf bereits vorhandenen oder allgemeinen Verbindungsinformationen beruht.

Datenschutzrechtliche Bewertung

Datenschutzrechtlich kommt es darauf an, welche Datenverarbeitung tatsächlich stattfindet. Ein Zugriff auf den präzisen Gerätestandort ohne App-Nutzung wäre problematisch und von der Einstellung „Während der Nutzung“ nicht gedeckt. Dafür fanden sich hier jedoch keine Anhaltspunkte.

Eine ungefähre Standortbestimmung über die IP-Adresse oder der Rückgriff auf bereits gespeicherte Ortsinformationen (z. B. eine zuletzt bekannte Stadt) ist hingegen in der Regel zulässig, sofern der Anbieter transparent informiert und bei werblichen Inhalten eine Abwahlmöglichkeit anbietet. Nach der DS-GVO gilt auch eine IP-basierte Ortsangabe als personenbezogenes Datum und erfordert eine Rechtsgrundlage – meist das berechtigte Interesse des Anbieters – sowie klare Information und die Möglichkeit, Direktwerbung zu widersprechen. Ein berechtigtes Interesse kann insbesondere dann angenommen werden, wenn die Standortbestimmung nur in grober Form erfolgt, keine zusätzlichen sensiblen Daten verarbeitet werden und der Zweck – etwa die Anzeige regional relevanter Angebote oder die Betrugsprävention – für den Nutzer erkennbar und verhältnismäßig ist und die die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen. Letzteres wäre anzunehmen, wenn aufgrund des Standorts beispielsweise Nutzungsprofile erstell werden würden.

Eine Einwilligung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) ist in diesem Fall nicht erforderlich, da die Zuordnung der IP-Adresse zum Standort serverseitig beim Anbieter erfolgt und keine Informationen vom Endgerät ausgelesen oder darauf gespeichert werden.

Reaktion des Betroffenen

Der Betroffene verstand die angezeigte Begrüßung als Hinweis darauf, dass sein aktueller Standort erfasst wurde, und ging davon aus, dass die iOS-Einstellung „Während der Nutzung“ solche Vorgänge vollständig ausschließt. Der Fall zeigt, wie leicht eine automatische, ortsbezogene Mitteilung – die technisch gesehen ohne aktive Standortabfrage auf dem Gerät funktioniert – als übergriffig wahrgenommen wird. Häufig wird dabei übersehen, dass die iOS-Berechtigungen sich nur auf den Zugriff auf die Sensoren des Geräts (z. B. GPS oder WLAN) beziehen, nicht jedoch auf serverseitige Rückschlüsse, die etwa aus der IP-Adresse oder bereits gespeicherten Kontoinformationen gezogen werden.

Fazit und Einordnung

Im Ergebnis ließ sich nachvollziehen, dass die beobachtete Mitteilung technisch auch ohne Zugriff auf präzise Standortdaten ausgelöst werden kann. Sie kann auf einer allgemeinen Standortbestimmung über die Internetverbindung oder auf bereits vorhandenen Angaben aus einer früheren Nutzung beruhen. Der Fall zeigt, dass bei mobilen Anwendungen leicht der Eindruck entstehen kann, das Gerät werde im Hintergrund geortet, obwohl solche Meldungen oft auf technischen Abläufen beruhen, die lediglich einen allgemeinen Bezug zum Standort herstellen.

Die Beschwerde zeigt, dass die Bewertung solcher Vorgänge ein genaues Verständnis der jeweiligen technischen Abläufe erfordert. Nur wenn klar zwischen lokal auf dem Gerät erhobenen Standortdaten und serverseitigen Informationen unterschieden wird, lässt sich eine sachgerechte Einschätzung vornehmen. Zugleich unterstreicht der Fall die Bedeutung transparenter Hinweise der Anbieter, um Fehlinterpretationen bei Nutzerinnen und Nutzern zu vermeiden.

5.6.3. Phishing statt Datenschutzverstoß: Gefälschte Mitteilung täuschte Datenleck vor

Art. 57 Abs.1 Buchst. a), f) DS-GVO

Im Jahr 2025 ging bei uns eine Beschwerde ein, die sich mit einem mutmaßlichen Datenschutzvorfall bei einem digitalen Bestellservice befasste. Die betroffene Person hatte im Zusammenhang mit einer früheren Essensbestellung über einen Lieferdienst eine E-Mail erhalten, die sie auf ein angebliches Datenleck hinwies. In dieser Nachricht wurde behauptet, dass der Lieferdienst fehlerhafte Software verbreite, ein Datenleck vorliege und personenbezogene Daten der betroffenen Person betroffen seien. Als Beleg enthielt die Beschwerde einen Ausschnitt mit personenbezogenen Daten und den Hinweis, dass sich das Unternehmen bislang nicht zurückgemeldet habe.

Die Beschwerde bezog sich insbesondere auf die Tatsache, dass die betroffene Person seither vermehrt unerwünschte Werbeanrufe (sog. Spam-Anrufe) erhalte und einen Zusammenhang mit dem angeblichen Datenleck herstellte. Die betroffene Person hatte im Rahmen der Bestellung unter anderem ihre Mobilnummer, E-Mail-Adresse und Wohnanschrift angegeben.

Analyse: E-Mail-Inhalt und technische Struktur der angeblichen Benachrichtigung

Im Zuge der Prüfung stellten wir fest, dass es sich bei der benannten Nachricht nicht um eine Mitteilung von einem Anbieter, sondern um eine gezielte Phishing-Nachricht handelte. Phishing bezeichnet den Versuch, über gefälschte Kommunikationswege an persönliche Daten zu gelangen oder gezielt Verunsicherung auszulösen. Im vorliegenden Fall wurde die betroffene Person per E-Mail kontaktiert, wohl von einer bestimmten Adresse, die jedoch mittels sogenanntem „E-Mail-Spoofing“ leicht zu fälschen ist.

Besonders auffällig war, dass die Nachricht nicht direkt auf eine Website verwies, sondern einen Link zu einem WhatsApp-Kontakt enthielt. Die betroffene Person nahm über diesen Link Kontakt auf – in der Annahme, mit dem Anbieter zu kommunizieren – und erhielt dort die Mitteilung, der Datenschutzbeauftragte sei informiert worden. Tatsächlich dürfte es sich hierbei bereits um einen gefälschten Chatkontakt gehandelt haben, der gezielt auf Glaubwürdigkeit ausgelegt war.

Im weiteren Verlauf wurde die betroffene Person offenbar zur Eingabe personenbezogener Daten verleitet. Die Nachricht und der gefälschte Kontakt zielten erkennbar darauf ab, Vertrauen zu erschleichen und eine Reaktion zu provozieren – ein bekanntes Muster bei Phishing-Angriffen.

Datenschutzrechtliche Bewertung

Aus datenschutzrechtlicher Sicht lag zum Zeitpunkt der Beschwerde kein meldepflichtiger Vorfall nach Art. 33 DS-GVO vor, wonach eine Verletzung des Schutzes personenbezogener Daten unverzüglich vom Verantwortlichen zu melden ist. Zwar war der betroffenen Person ein personenbezogenes Dokument zugegangen, dieses jedoch nicht durch den Anbieter selbst, sondern durch eine nicht verifizierbare externe Quelle. Auch konnten keine Hinweise darauf gefunden werden, dass ein unbefugter Zugriff auf Systeme des Lieferdienstes erfolgt war oder personenbezogene Daten von dort aus unrechtmäßig weitergegeben wurden.

Nach der Prüfung liegt kein Datenschutzverstoß durch das Unternehmen vor. Die erhaltene Nachricht erfüllt nicht die Kriterien eines Verstoßes im Sinne von Art. 4 Nr. 12 DS-GVO, da keine Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten durch die verantwortliche Stelle erfolgt ist. Die im Rahmen der Phishing-Nachricht erfolgte Verwendung personenbezogener Daten (z. B. Name, E-Mail-Adresse) ist vielmehr einer unbefugten Handlung eines Dritten zuzurechnen und nicht einer Verarbeitung durch den Verantwortlichen.

Empfehlung an die betroffene Person

Die betroffene Person wurde von uns über die Täuschungsabsicht der E-Mail informiert und auf die Merkmale von Phishing-Nachrichten hingewiesen. Zudem wurde erläutert, dass die empfangene Nachricht keine legitime Mitteilung des Unternehmens darstellt und keine Kommunikation mit Servern des Anbieters stattgefunden habe. Als Vorsichtsmaßnahme haben wir empfohlen:

- keine Anhänge oder Links aus der Nachricht zu öffnen
- die E-Mail zu löschen
- Passwörter zu ändern (insbesondere sofern dieselben Zugangsdaten auch an anderer Stelle verwendet werden)
- sowie eine Prüfung der Endgeräte auf potenzielle Schadsoftware vorzunehmen

Des Weiteren haben wir den Hinweis gegeben, dass Werbeanrufe auch auf anderen Wegen zustande kommen können, etwa durch den Weiterverkauf von Daten durch Drittanbieter oder durch vorherige Einwilligungen an anderer Stelle.

Fazit und Einordnung

Dieser Fall zeigt exemplarisch, wie leicht technische Nachrichten über Datenpannen oder Sicherheitsvorfälle missverstanden oder sogar gezielt missbraucht werden können, um Unsicherheit zu erzeugen. Die durchgeführte Analyse konnte einen tatsächlichen Datenschutzverstoß ausschließen und stattdessen auf ein durch Phishing verursachtes Sicherheitsproblem hinweisen, das außerhalb der Verantwortung des genannten Anbieters lag. Eine datenschutzrechtliche Maßnahme war daher nicht erforderlich. Gleichwohl macht der Fall deutlich, wie wichtig Aufklärung und technische Medienkompetenz sind, um reale von vermeintlichen Vorfällen unterscheiden zu können.

Auch wenn der vorgebliche Absender nicht verantwortlich ist, kann es oft sinnvoll sein, die Kundinnen und Kunden auf einen solche Betrugsmasche hinzuweisen um diese dadurch zu sensibilisieren und auch sich selbst vor unberechtigten Vorwürfen zu schützen.

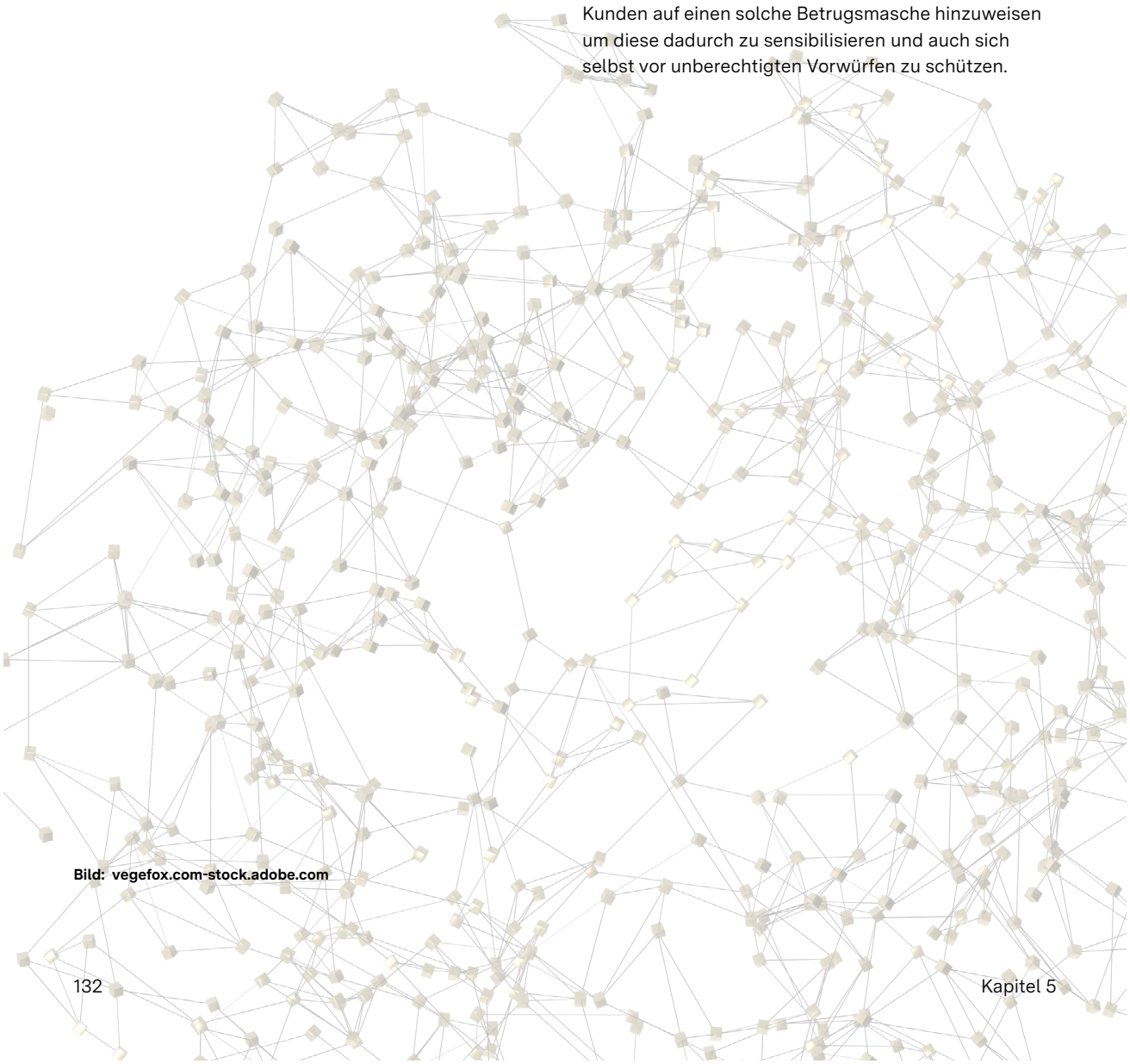


Bild: vegefox.com-stock.adobe.com

5.6.4. Löschung von personenbezogenen Daten in den Suchergebnissen von Suchmaschinen

57 Abs.1 Buchst. a), f) DS-GVO

Uns erreichte 2025 eine Vielzahl von Beschwerden, die die Offenlegung personenbezogener Daten in den Suchergebnissen von Suchmaschinen, insbesondere Google, zum Gegenstand haben. Ausgangspunkt ist, dass die personenbezogenen Daten auf einer bestimmten Internetseite offengelegt wurden, meist innerhalb eines Textes oder in einem Dokument, das auf dieser Internetseite verfügbar ist. Auch nach erfolgreicher Löschung dieser Daten erscheinen weiterhin Auszüge des Beitrags oder Dokuments in den Google-Suchergebnissen, die personenbezogene Daten der betroffenen Person enthalten.

Der Hintergrund

Nicht in jedem Falle besteht bei einer Namensnennung im Internet ein Anspruch auf Löschung gemäß DS-GVO. So unterliegen Verarbeitungen personenbezogener Daten zu journalistischen Zwecken grundsätzlich im Wesentlichen nur hinsichtlich der Sicherheit der Verarbeitung der DS-GVO (vgl. Art. 85 DS-GVO in Verbindung mit § 12 Landespressegesetz bzw. § 12 Medienstaatsvertrag). Dies stellt sicher, dass wir als staatliche Aufsichtsbehörde keine Kontrolle von Meinungen oder journalistischen Beiträgen durchführen. Betroffene haben aber die Möglichkeit, zivilrechtlich im Rahmen des allgemeinen Äußerungsrechts gegen unwahre Tatsachenbehauptungen vorzugehen oder bei Überschreitung strafrechtlicher Grenzen (wie Beleidigungen, übler Nachrede oder Verleumdungen) die Strafverfolgungsbehörden einzuschalten.

Uns begegnet auch die Situation, dass die von einer Äußerung betroffene Person nicht direkt die Entfernung des betreffenden Inhalts fordert, sondern nur die Entfernung aus Suchmaschinen. Im Rahmen der Abwägung, ob eine solche Löschung gerechtfertigt ist, sind allerdings neben den Persönlichkeitsrechten der Betroffenen auch die unternehmerische Freiheit der Suchmaschinenbetreiber, die Grundrechte der jeweiligen Inhalteanbieter sowie die Informationsinteressen der Internetnutzer zu berücksichtigen (vgl. Beschluss des Bundesverfassungsgerichts vom 6. November 2019, 1 BvR 276/17, „Recht auf Vergessen II“).

Für betroffene Personen ist es daher in der Regel ratsam, ein Recht auf Löschung bei der Original-Quelle zu erreichen, wenn ein solcher Anspruch besteht. Ein Beispiel für häufige Fälle ist die Nennung von Klartext-Namen im Rahmen von Antworten auf von unter Pseudonym abgegebenen Rezensionen von Restaurants, Anwält_innen, Ärzt_innen oder anderen Dienstleister_innen. Solche ungewollten Namensnennungen stellen grundsätzlich einen DS-GVO-Verstoß dar und Betroffene haben gegenüber den Autor_innen und Plattformbetreibern einen Lösch-Anspruch.

Nach erfolgter Löschung kommt es aber oft weiterhin zu einer Auffindbarkeit von Textschnippseln (Snippets) in Suchmaschinen wie Google.

Ein Snippet ist eine Beschreibung oder Zusammenfassung eines Suchergebnisses in der Ergebnisliste einer Online-Suche. Hier werden die wichtigsten Informationen über den zur Suche passenden Inhalt der entsprechenden Internetseite zusammengefasst mit dem Ziel, diejenigen Seiteninhalte hervorzuheben, die für die Suche eines Nutzers am relevantesten sind. Der Inhalt des Snippets wird automatisch anhand der Inhalte auf der Internetseite durch den Suchmaschinenbetreiber bestimmt. Eine manuelle Änderung wird durch die Suchmaschinen nicht vorgenommen.

Wir haben uns häufig mit zwei Konstellation befasst: Erstens, die gelöschten personenbezogenen Daten waren ein Teil einer Seite, die aber weiterhin existiert, aus der aber beispielsweise eine Zeile einer Tabelle oder ein Absatz entfernt wurde. Oder zweitens, die Seite mit den personenbezogenen Daten wurde im Ganzen von der verantwortlichen Stelle entfernt. In beiden Fällen können jedoch die Daten immer noch im Snippet bei der entsprechenden Google-Suche sichtbar sein, teilweise auch lange nach der Löschung auf der Ursprungsseite.

Der Grund dafür ist, dass der angezeigte Inhalt des Snippets durch die Suchmaschine automatisch anhand der Inhalte auf der Internetseite bestimmt wird, und in diesem Fall die Änderung der Inhalte auf der Internetseite der Suchmaschine noch nicht bekannt ist. Der Prozess, Inhalte auf Internetseiten automatisch durchzusuchen, wird auch „Crawling“ genannt. Eine Software wie beispielsweise der Googlebot crawlt regelmäßig das Internet und versucht alle Inhalte zu finden, um

die Informationen aus den gefundenen Seiten abzuspeichern und anhand dieser Informationen die eigene Datenbank, den sog. Suchmaschinen-Index, zu aktualisieren. Dieser Prozess wird daher auch Indexierung genannt. Bei der entsprechenden Suche eines Nutzenden wird auf diese Datenbank zurückgegriffen, und relevante Informationen für die Suche herausgesucht und dem/der Nutzenden dementsprechend angezeigt.

Dieses Crawling kann in verschiedenen Zeitabständen geschehen: manche Webseiten werden durch Google mehrmals am Tag aktualisiert, andere über Wochen oder Monate gar nicht, insbesondere selten aufgerufene Unterseiten oder solche, die in der Vergangenheit selten aktualisiert wurden.

Was betroffene Personen tun können

Als allererstes raten wir betroffenen Personen bei berechtigten Löschanliegen dazu, bei der verantwortlichen Stelle (also dem Betreiber des betreffenden Internetangebots) die Löschung der entsprechenden personenbezogenen Daten zu verlangen.

Wir empfehlen, die genauen Adressen aller betroffenen Inhalte konkret zu nennen. Erfahrungsgemäß kommt es durchaus vor, dass die Verantwortlichen zwar die Datei entfernt haben, ihnen jedoch nicht bewusst ist, wenn weitere Kopien noch vorhanden sind und bei einer Suche weiterhin erscheinen. In solchen Fällen ist es hilfreich, dass betroffene Personen gleich bei der Löschungsanfrage alle Fundstellen nennen, aber auch nach einer Löschungsbestätigung der verantwortlichen Stelle durch eine erneute Suche prüfen, ob wirklich alle relevanten Daten entfernt wurden.

In den meisten Fällen wird die Löschung bzw. die entsprechende Änderung der Internetseite der Suchmaschine nicht sofort bekannt. Die Indexierung durch Suchmaschinen erfolgt jedoch regelmäßig, weshalb wir betroffenen Personen grundsätzlich raten abzuwarten, bis die Suchmaschine den Index aktualisiert hat und die personenbezogenen Daten damit auch nicht mehr im Snippet erscheinen.

Sollte dies nach einigen Wochen noch immer nicht der Fall sein, sollte die betroffene Person erst einmal prüfen, ob wirklich alle Quellen, die ihre personenbezogenen Daten beinhalten, bereits von der verantwortlichen Stelle gelöscht sind, indem sie die entsprechenden Suchergebnisse aufruft. Ist die Internetseite oder die Datei, die in der Suche verlinkt ist, nicht mehr verfügbar bzw. der betreffende Inhalt nicht mehr enthalten, ist davon auszugehen, dass diese tatsächlich entfernt wurde. Betroffene können dann von dem Verantwortlichen verlangen, eine sofortige Re-Indexierung bei der Suchmaschine zu beantragen. Sollte der zu löschende Inhalt unter neuer Adresse immer noch vorhanden sein, ist es ratsam, genau diese Adresse der verantwortlichen Stelle zu nennen. In diesem Fall kann die betroffene Person nach der Wartezeit die Entfernung ihrer persönlichen Daten bei der Suchmaschine beantragen. Sollte dies auch ohne Erfolg sein, empfehlen wir Betroffenen eine Beschwerde bei uns einzureichen.

5.6.5. Doxing in sozialen Medien: Content Creator wurde verwarnt

57 Abs.1 Buchst. a), f) DS-GVO

Im Jahr 2025 haben wir einen Content Creator verwarnt. Der Verwarnung ging eine Beschwerde voraus, die die Veröffentlichung von Videoaufnahmen zum Gegenstand hat. Die Beschwerde richtete sich gegen einen Content Creator, der bei einer unerfreulichen Begegnung mit der betroffenen Person Videoaufnahmen gemacht und anschließend diese Videoaufnahmen auf der persönlichen Seite auf der Social Media Plattform veröffentlicht hat.

Diese Videoaufnahmen waren mindestens 24 Stunden den Followern dieses Content Creators öffentlich zugänglich (zum Zeitpunkt unserer Prüfung hatte er bereits eine mittlere fünfstellige Anzahl an Followern). In einem der Videos äußerte er die Hoffnung, dass jemand die betroffene Person in den weiteren veröffentlichten Videos erkennen und ihm ihren Namen nennen könne. In dem entsprechenden Beitrag war

Infokasten

Eine genaue Erklärung über Betroffenenrechte sowie weitere Hilfestellung inkl. Mustervorlagen finden betroffene Personen auf unserer Homepage unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/03/Betroffenenrechte.pdf.

die betroffene Person, das Kfz-Kennzeichen eines vor ihrem Wohnhaus stehenden Fahrzeugs und die Briefkastenanlage ihres Wohnhauses, auf der Namen der Bewohner zu erkennen sind, der Öffentlichkeit zugänglich.

Das Veröffentlichen der Videoaufnahmen, in denen die betroffene Person eindeutig zu sehen ist, in Verbindung mit der Veröffentlichung ihres Wohnhauses sowie der dazugehörigen Namenschilder erfolgte ohne Rechtsgrundlage und hat die betroffene Person in ihrem Recht auf informationelle Selbstbestimmung verletzt. Die Veröffentlichung der genannten Informationen auf der Social-Media-Seite war mangels einer Einwilligung nach Art. 6 Abs.1 Buchst. a) DS-GVO oder eines überwiegenden berechtigten Interesse nach Art. 6 Abs.1 Buchst. f) DS-GVO unzulässig.

Aufgrund der hohen Anzahl an Followern kann man davon ausgehen, dass die Beiträge des Content Creators die breite Öffentlichkeit erreichen, auch wenn sie nur für eine kurze Zeit online verfügbar sind. Die Veröffentlichung des Beitrags auf der eigenen Social-Media-Seite stellt eine Datenverarbeitung im Sinne von Art. 4

Nr. 2 DS-GVO dar, nämlich eine Offenlegung.

Nach Art. 6 Abs.1 DS-GVO ist die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn mindestens eine der insgesamt sechs im Einzelnen in Buchst. a) bis f) dieser Vorschrift aufgeführten Voraussetzungen erfüllt ist. Es liegt jedoch in solchen Fällen in der Regel weder eine Einwilligung der betroffenen Person noch ein Vertrag mit dieser vor.

Auch kommt kein überwiegendes, berechtigtes Interesse nach Art. 6 Abs.1 Buchst. f) DS-GVO in Betracht. Das Zeigen des Gesichts der betroffenen Person in Verbindung mit der Veröffentlichung ihres Wohnhauses, der Namen auf der Briefkastenanlage dieses Wohnhauses oder ihres Kfz-Kennzeichens kann nicht mit einem berechtigten Interesse begründet werden. Hierbei geht es nicht um eine Meinungsäußerung im Zusammenhang mit der Begegnung, denn die genannten Informationen hatten und haben nichts mit der Auseinandersetzung zu tun und waren zu keinem Zeitpunkt für die Meinungsbildung in der Öffentlichkeit erforderlich.

Insgesamt erfolgte die Veröffentlichung der entsprechenden Videoaufnahmen ohne Rechtsgrundlage und war somit unzulässig. Wer Bildaufnahmen von Begegnungen mit Dritten im Internet veröffentlichen will, sollte grundsätzlich die Einwilligung der betroffenen Personen einholen, oder diese so unkenntlich machen, dass sie nicht wiedererkannt werden können. Dies gilt nicht für journalistische Tätigkeiten, z. B. bei Aufnahmen von öffentlichen Versammlungen wie Demonstrationen oder Karnevalsumzügen. Eine Veröffentlichung solcher Aufnahmen ist grundsätzlich (in den Grenzen der allgemeinen Gesetze) zulässig.

5.6.6. Tracking in Apps

Art. 57 Abs.1 Buchst. a), b), d), f) DS-GVO

Im vergangenen Jahr haben wir der Anbieterin einer App den Einsatz von Google Analytics untersagt. Die App, die den Dienst Google Analytics ohne vorherige, freiwillige, informierte, aktiv und separat von anderen Erklärungen abgegebene und jederzeit widerrufliche Einwilligung der betroffenen Personen gemäß Art. 6 Abs.1 Buchst. a), Art. 7 und Art. 4 Nr. 11 DS-GVO nutzte, hat gegen die Datenschutz-Grundverordnung verstoßen, da sie ohne Rechtsgrundlage Nutzendendaten an Google Analytics übermittelte.

Die Untersuchung der App ergab Mängel bei der Nutzung des Drittdienstes Google Analytics bereits bevor der App-Nutzer mit der App überhaupt agiert. Die Untersuchung in unserem hauseigenen Prüflabor zeigte insbesondere, dass die Betreiberin der App über eine Einbindung dieses Drittdienstes Informationen über das verwendete Gerät und weitere Daten an Google Analytics übermittelt.

Zu den zahlreichen erfassten Daten gehörten die für das Gerät speziell vergebene Kennung und die IP-Adresse des Geräts des Nutzers. Wir wiesen in einem Anhörungs-Schreiben den App-Betreiber auf unsere Untersuchungsergebnisse hin. Hinsichtlich Google Analytics vertrat der App-Betreiber trotz unserer Hinweise die Auffassung, Google Analytics werde zum Zwecke der eingeschränkten Überwachung der ordnungsgemäßen Funktion des App-Starts eingesetzt. Diese Auffassung teilten wir nach eingehender Prüfung nicht, woraufhin eine Untersagung und die Anordnung der Löschung aller ohne Rechtsgrundlage erhobenen Daten erfolgte. Die Überwachung der Funktionsfähigkeit des App-Starts und der App im Allgemeinen ist zwar ein berechtigtes Interesse der App-Betreiberin. Zur Wahrung dieses Interesses ist es jedoch nicht

Bild: bakhtiarzein-stock.adobe.com

erforderlich, Google Analytics einzusetzen. Der Einsatz von Google Analytics zur Überwachung des App-Starts ist technisch nicht geeignet, da Google Analytics hauptsächlich für die Analyse von Nutzendenverhalten und nicht für die Erfassung technischer Systemmetriken entwickelt wurde.

Die Maßnahme erwies sich als erfolgreich. Die Betreiberin der App hat die Maßnahme akzeptiert und die notwendigen Nachbesserungen umgesetzt. Eine erneute Prüfung konnte die Umsetzung bestätigen. Auch hat die Betreiberin uns gegenüber Nachweise geliefert, die bereits an Google Analytics übermittelten Daten bei diesem Dienst gelöscht zu haben.

Aus diesem Anlass wollen wir alle in Baden-Württemberg ansässigen App-Betreiber_innen auf die rechtskonforme Einbindung von Drittdiensten hinweisen. Der Einsatz von Google Analytics geht in vielen Fällen mit der Speicherung von einer Kennung oder dem Auslesen von Informationen des Endgeräts einher, welche dann wiederum an Server von Google übermittelt werden. Eine solche Verarbeitung unterliegt den Anforderungen der DS-GVO und von § 25 TDDDG und ist in der Regel einwilligungsbedürftig. Wir arbeiten derzeit an einer Handreichung für App-Betreiber_innen und werden sie hoffentlich bald veröffentlichen können.

5.6.7. Tracking im Internet: Cookieless-Tracking braucht eine Rechtsgrundlage

Art. 57 Abs.1 Buchst. a), b), d), f) DS-GVO

In einem Fall haben wir im Jahr 2025 einem Webseitenbetreiber den Einsatz von verschiedenen Analyse-Diensten untersagt und ihn angewiesen, bereits übermittelte Daten der Nutzenden beim jeweiligen Dienste-Anbieter löschen zu lassen.

Hier konnten wir beobachten, dass der Webseitenbetreiber keine Cookies einsetzen. Das Tracking fand vielmehr über spezifische Merkmale des Browsers oder des Geräts statt. Hier werden bestimmte Eigenschaften bzw. Einstellungen des Browsers oder des Geräts an Server des Drittdienstes übermittelt. Dem bzw. der jeweiligen Nutzenden wird eine individuelle ID vergeben, die zusammen mit weiteren Browser- und Geräteinformationen an die Drittdienste übermittelt werden. Somit lassen sich die Nutzenden in allermeisten Fällen doch eindeutig identifizieren. Allein

die Übermittlung dieser Daten stellt eine Verarbeitung personenbezogener Daten dar, die einer Rechtsgrundlage nach DS-GVO bedarf. Wir konnten in diesem Fall keine wirksame Einwilligung feststellen, da kein Einwilligungsbanner vorhanden war. Auch war von einem überwiegenden berechtigten Interesse nicht auszugehen.

Uns war in diesem Fall bewusst, dass Anbieter_innen von Internetangeboten, insbesondere kleine Unternehmen, zum Teil erhebliche Schwierigkeiten mit der technischen Umsetzung ihres eigenen Internetauftritts haben. Es ist durchaus gängige Praxis, dass Unternehmen für die Erstellung oder Ausgestaltung ihrer Internetseite Baukastensysteme nutzen, oder externe Dienstleister beauftragen. Aus diesem Grund haben wir nach unseren Anordnungen aktiv Kontakt mit dem Webseitenbetreiber gesucht und ihn auch nochmals die technischen sowie rechtlichen Gegebenheiten erklärt. Auch haben wir besonders darauf hingewiesen, dass datenschutzrechtlich Verantwortlicher nach Art. 4 Nr. 7 DS-GVO nicht das Unternehmen ist, das den Baukasten bereitstellt, oder der IT-Dienstleister, der die Webseite erstellt hat oder aktuell betreut.

Dieses sind grundsätzlich Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO). Verantwortlicher ist in den meisten Fällen der Webseitenbetreiber selbst. Diesen treffen die Pflichten nach DS-GVO und TDDDG. Der Webseitenbetreiber hat also dafür zu sorgen, dass Verarbeitungen, die auf oder aufgrund seiner Webseite stattfinden, den Anforderungen des TDDDG und der DS-GVO genügen. Dazu zählt insbesondere die Pflicht, sicherzustellen, dass aus Nutzendenperspektive nicht-notwendige Cookies unterbleiben sowie etwaige Verarbeitungen personenbezogener Daten auf eine wirksame Rechtsgrundlage stützten.

Der Webseitenbetreiber hat unsere Anordnungen akzeptiert und seine Internetseite nachgebessert, so dass alle von uns genannten Mängel nunmehr behoben wurden.

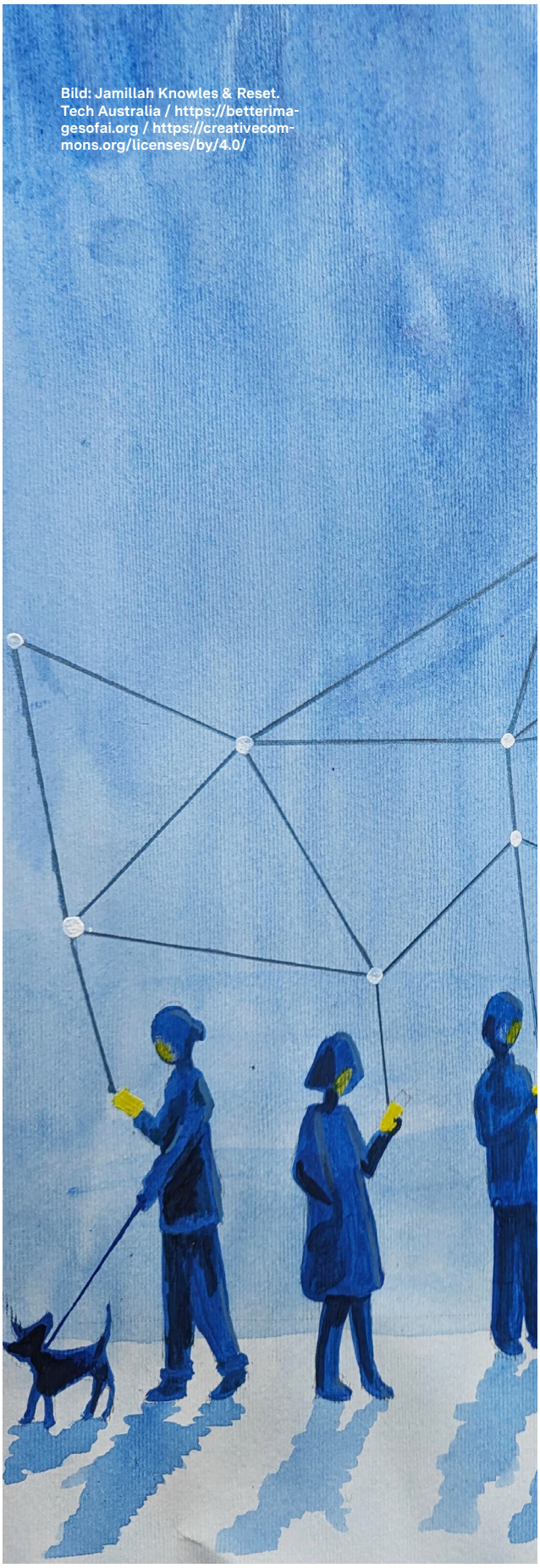
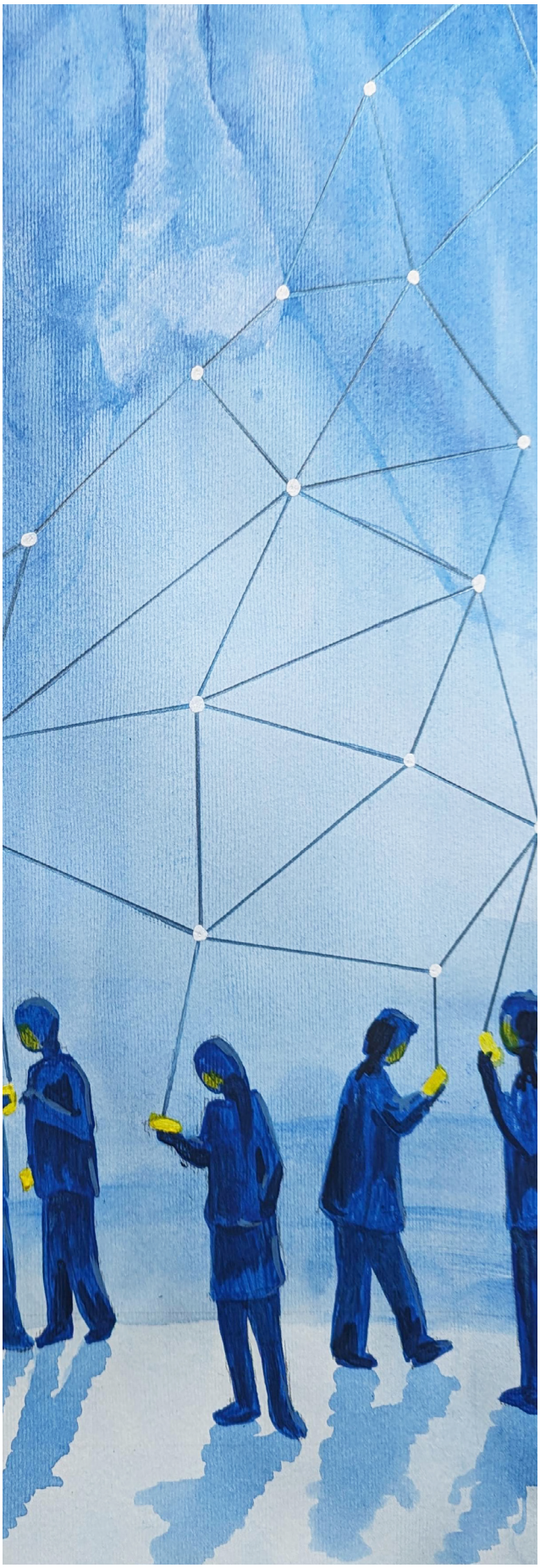


Bild: Jamillah Knowles & Reset. Tech Australia / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/



5.6.8. Tracking in E-Mails: datenschutzfreundliche Alternativen zur Erfolgskontrolle ohne Personalisierung

Art. 57 Abs.1 Buchst. a), b), d), f) DS-GVO

In diesem Jahr erreichten uns mehrere Beschwerden betreffend Tracking in E-Mails. In einem Fall haben wir ein Unternehmen wegen des Trackings in E-Mails verwarnt.

Im Bereich des E-Mail-Marketings, bei Newslettern und Ähnlichem werden oftmals verschiedene Techniken verwendet, die es dem Absender erlauben nachzuvollziehen, welcher Empfänger wann die E-Mail erhalten und gelesen hat, mit welchem Gerät die E-Mail gelesen wurde, wo sich die Person aufgehalten und welche Links sie aufgerufen hat.

Dazu werden in den verschickten HTML-Emails Anweisungen für das Nachladen externer Elemente wie kleiner, für jeden Empfänger individueller Bilder (Tracking-Pixel) eingebaut. Beim Lesen und teilweise bereits beim Empfang der E-Mail werden diese Bilder durch viele (nicht alle) E-Mail-Programme oder Webmailer vom Tracking-Server nachgeladen und dieser kann dann genau nachvollziehen, wer die E-Mail wann (und anhand der IP-Adresse auch grob wo) gelesen hat. Zudem sind auch Links in solchen Mails oftmals pro Empfänger individuell, so dass auch hier nachvollzogen werden kann, wer genau welchen Link aufgerufen hat.

Damit ist es also sehr detailliert möglich, das individuelle E-Mail-Leseverhalten nachzuvollziehen und zu überwachen. Nach DS-GVO kommt dafür als Rechtsgrundlage grundsätzlich nur die informierte und freiwillige sowie aktiv und separat von anderen Erklärungen abgegebene Einwilligung in konkret diese Überwachung in Betracht. Eine generelle Einwilligung in den Empfang von Newsletter und ggf. ein Hinweis auf Datenschutzinformationen nach Art. 13 DS-GVO ist dafür nicht ausreichend, sondern die Empfänger müssen explizit der Überwachung ihres E-Mail-Leseverhaltens zustimmen.

Je nach genauer Implementierung ist es in der Regel bereits notwendig, eine Einwilligung nach § 25 TDDDG

einzuholen, da die externen Tracking-Pixel im Cache (Zwischenspeicher) des E-Mail-Programms oder Browsers gespeichert werden, was eine Speicherung im Sinne des § 25 Abs.1 Satz 1 TDDDG darstellt. Die Einbindung der Bild-Datei dient lediglich der Protokollierung des Lesens der E-Mail und keinen anderen Zwecken. Sie ist also nicht (technisch) unbedingt erforderlich für das Anzeigen der vom Nutzenden gewünschten Inhalte. Die Speicherung wird also nicht vom Ausnahmetatbestand des § 25 Abs. 2 Nr. 2 TDDDG erfasst und bedarf daher einer Einwilligung.

Verantwortliche wollen jedoch oftmals keine einzelnen Personen individuell überwachen, sondern nur mittels sog. A/B-Tests herausfinden, ob bestimmte Formulierungen oder Varianten eines Newsletters bei den Empfängern besser ankommen. Zu diesem Zweck ist der Versand von Mails mit personenscharf individuellen Links nicht notwendig.

Wir empfehlen, Mails mit unterschiedlichen Links zu versenden, die sich aber für jede Gruppe unterscheiden. So können Verantwortliche anhand der Anzahl der Aufrufe für den jeweiligen Link nachvollziehen, welche E-Mail-Variante besser ankommt.

Beispiel:

Angenommen, der normale Link lautet: https://www.example.com/info/aktuelle-meldung.html

Um zählen zu können, wie viele Empfänger des Newsletters dem Link folgen könnte im Newsletter eine eigene Adresse verwendet werden, aber bei allen Empfängern die gleiche: https://mailing.example.com/info/aktuelle-meldung.html oder https://www.example.com/mail/aktuelle-meldung.html

Um zusätzlich A/B-Testing zu machen, also um zu zählen, welcher Wortlaut des Newsletters erfolgversprechender ist, könnte zusätzlich folgende Anpassung verwendet werden: https://mailing.example.com/a/aktuelle-meldung.html und https://mailing.example.com/b/aktuelle-meldung.html

Damit ist es möglich, sowohl die Nutzerinnen und Nutzer der Webseite zu zählen, die über den Newsletter die Seite aufrufen als auch eine Erfolgsmessung verschiedener Varianten durchzuführen. Wir hoffen, dieser praktische Service-Tipp hilft allen Beteiligten. Wir behalten das Thema weiter im Blick.

5.6.9. Einwilligungsbanner um jeden Preis? Warum ein unnötiges Einwilligungsbanner Probleme bereitet

Art. 57 Abs.1 Buchst. a), f) DS-GVO

In diesem Jahr erreichten uns zahlreiche Beschwerden, die sog. „Cookie-Banner“ betreffen. Darin wird meist bemängelt, dass das Banner keine Möglichkeit enthält, die nicht notwendigen Cookies abzulehnen.

In einigen Fällen haben wir nach technischer Untersuchung der jeweiligen Internetseite festgestellt, dass keine einwilligungsbedürftige Verarbeitung stattfindet und somit kein Einwilligungsbanner notwendig ist, oder nur notwendige Cookies wie das Speichern der Auswahl im Cookie-Banner nach Interaktion durch die Nutzenden stattfindet – für die wiederum keine Einwilligung erforderlich wäre –, oder die einzige einwilligungsbedürftige Verarbeitung der Cookie vom Cookie-Banner selbst ist, der aber bereits vor Interaktion der Nutzenden mit dem Banner und damit vor der Einwilligung gesetzt wird und damit ohne – in diesem Fall erforderliche – Einwilligung genutzt wird.

Eine Einwilligung ist dort erforderlich, wo eine einwilligungsbedürftige Verarbeitung stattfindet. Dies ist in aller Regel der Fall, wenn Daten auf dem Endgerät von Nutzenden gespeichert werden oder auf bereits im Endgerät gespeicherte Daten zugegriffen werden oder wenn personenbezogene Daten verarbeitet werden, für die als Rechtsgrundlage nur die Einwilligung möglich ist.

Nach TDDDG ist keine Einwilligung nötig, wenn nur Informationen auf den Endgeräten der Nutzenden abgelegt oder von dort ausgelesen werden, die unbedingt erforderlich sind, damit von den Nutzenden ausdrücklich gewünschte Dienste zur Verfügung gestellt werden können (dies kann zum Beispiel eine Warenkorb-Funktion oder ein Login sein). Auch eine Einwilligung für die nachfolgende Verarbeitung nach DS-GVO ist nicht erforderlich, soweit keine einwilligungsbedürftigen Verarbeitungen vorgenommen werden, z. B. wenn die nachfolgende Datenübermittlung sich auf eine andere Rechtsgrundlage stützt als

die Einwilligung. Ein Einwilligungsbanner suggeriert Nutzenden der Internetseite fälschlicherweise, es fänden auf der Internetseite einwilligungsbedürftige Verarbeitungen statt, in die sie die Wahl hätten einzuwilligen. Aus diesem Grund empfehlen wir, soweit die Datenverarbeitung keiner Einwilligung bedarf, kein Einwilligungsbanner einzusetzen. Betroffenen zu suggerieren, sie könnten ihre Einwilligung widerrufen, obwohl dies gar nicht der Fall ist (also eine andere Rechtsgrundlage als die Einwilligung herangezogen wird), verstößt gegen die Grundsätze von Treu und Glauben sowie der Transparenz, da es sich um eine falsche und irreführende Information handelt (vgl. Art. 5 Abs.1 DS-GVO sowie Art. 12 Abs.1 in Verbindung mit Art. 13 Abs. 2 Buchst. c) DS-GVO).

5.6.10. Datenleck bei zahlreichen Feuerwehren offenbart Mängel bei Löschprozessen

Art. 57 Abs.1 Buchst. a), d), h) DS-GVO

Wir mussten uns im vergangenen Jahr mit einem Sicherheitsvorfall in einer Feuerwehr-Software befassen. Wir haben den Vorfall intensiv aufgearbeitet – und betroffene Gemeinden haben Maßnahmen für die Zukunft getroffen.

Durch ein Sicherheitsleck kam zutage, dass es bei vielen Städten und Gemeinden einigen Nachbesserungsbedarf gab in Bezug auf Löschprozesse, aber auch im korrekten Umgang mit Datenschutzverletzungen. Letztlich hätte eine bei den Städten und Gemeinden bereits in der Vergangenheit praktizierte konsequente Routine, nicht mehr benötigte Daten von Feuerwehrleuten systematisch zu löschen, das gesamte Ausmaß des Sicherheitslecks deutlich begrenzt.

Aber der Reihe nach: Was war passiert? Uns hatte ein Sicherheitsforscher auf ein Datenleck einer Feuerwehr-Software aufmerksam gemacht, dessen Aufarbeitung und Verfolgung uns auch während des gesamten darauffolgenden Kalenderjahres 2025 intensiv beschäftigt hat. Das Leck stammte von einer Anbieterin, die eine Software für die Personal- und Einsatzplanung von Feuerwehren entwickelt hat und betreibt, welche insbesondere von vielen (Freiwilligen) Feuerwehren der Städte und Gemeinden in Baden-Württemberg genutzt wird.

Unseren Erkenntnissen zufolge hatte eine von der Software-Anbieterin fehlerhafte Einstellung zur Folge, dass über einen nicht genau bekannten Zeitraum Listen mit Links zu zahlreichen Dokumenten der Angehörigen der (Freiwilligen) Feuerwehr bei Kenntnis oder durch Erraten der entsprechenden URL eingesehen werden konnten. Dabei waren schätzungsweise insgesamt über 130.000 Dokumente mit personenbezogenen Daten von Feuerwehrleuten zahlreicher Städte und Gemeinden Baden-Württembergs online auffindbar, darunter z. B. Fortbildungsnachweise und Unfallberichte, aber auch sensiblere Dokumente wie etwa Führerschein- oder Ausweiskopien bis hin zu Kategorien besonderer personenbezogener Daten wie Corona-Tests und Krankmeldungen oder etwa einer Jahrzehnte zurückliegenden Disziplinarmaßnahme, die längst hätte gelöscht sein müssen. Nachdem wir die Software-Anbieterin ermittelt und über den Vorfall informiert haben, konnte sie dieses Leck am selben Abend schließen.

In Anbetracht dessen, dass wir aufgrund des uns durch den Sicherheitsforscher zugespielten Datenmaterials und -volumens davon ausgehen mussten, dass eine große Anzahl von Feuerwehren zahlreicher Städte und Gemeinden in Baden-Württemberg von dem Sicherheitsleck betroffen waren, hatte unsere Abteilung für technisch-organisatorischen Datenschutz und Datensicherheit ein individuell auf diese Datenschutzverletzung zugeschnittenes Datenpannen-Meldeformular entwickelt. Die erwarteten massenhaften Datenpannenmeldungen durch die für die (Freiwilligen) Feuerwehren verantwortlichen Städte und Gemeinden blieben im weiteren Verlauf zu unserer Verwunderung jedoch aus.

Also haben wir die insgesamt 166 Städte und Gemeinden Baden-Württembergs, die nach unseren Erkenntnissen von dem Sicherheitsvorfall betroffen waren, per allgemeinem Rundschreiben über das Datenleck informiert. In dem Rundschreiben haben wir den Städten und Gemeinden zudem mitgeteilt, unter welchen Voraussetzungen die Pflicht besteht, uns als Aufsichtsbehörde diese Datenpanne zu melden und betont, dass im Falle eines voraussichtlich hohen Risikos für die Rechte und Freiheiten der Feuerwehrleute diese darüber hinaus schriftlich benachrichtigt werden müssen.

Trotz unserer breit gestreuten Rund-E-Mail hatten uns bis Anfang April 2025 lediglich etwa 40 Städte und Gemeinden entsprechende Datenpannen im Zusammenhang mit dem Sicherheitsvorfall gemeldet.

Daraufhin haben wir das gesamte uns vorliegende Datenmaterial stichprobenartig gesichtet. Hierbei in Art oder Ausmaß „auffälliges" Datenmaterial haben wir im zweiten Schritt abgeglichen mit der uns von der Software-Anbieterin zur Verfügung gestellten internen Kundenliste. Zudem haben wir die Angaben der Städte und Gemeinden, die diese in ihren jeweiligen Datenpannenmeldungen gemacht haben, dem uns vorliegenden Datenmaterial gegenübergestellt. Auf diese Art und Weise haben wir aus dem Kreis aller betroffener Städte und Gemeinden letztlich vier Städte identifiziert, bei welchen aufgrund der Anzahl und/oder der Art der betroffenen Daten aufsichtsrechtliche Schritte durch uns geboten waren.

Diese vier Städte haben wir schließlich im Mai 2025 jeweils angeschrieben und diese über unsere Erkenntnisse informiert. Wir haben drei der vier Städte ferner aufgefordert, uns die Datenpanne zu melden und die vierte Stadt gebeten, ihre erste offensichtlich unvollständige Datenpannenmeldung zu ergänzen sowie die von dem Leck betroffenen Angehörigen der (Freiwilligen) Feuerwehr zu benachrichtigen.

Im Laufe unserer Ermittlungen hat sich aus den übereinstimmenden Aussagen der Städte uns gegenüber herausgestellt, was die (wahrscheinliche) Hauptursache war, dass die betroffenen Städte und Gemeinde größere Schwierigkeiten hatten, das Ob bzw. das Ausmaß der eigenen Betroffenheit aufzuklären.

Die Städte erkannten schließlich das konkrete Ausmaß ihrer eigenen Betroffenheit, kooperierten von da an alle grundsätzlich gut – mit unterschiedlicher Intensität – mit uns als Aufsichtsbehörde und lieferten uns ausführliche Darstellungen sowie detailliertere Einblicke in das Geschehene und Fehleranalysen. Im Ergebnis haben wir insgesamt gegen drei Städte jeweils Verwarnungsbescheide nach Art. 58 Abs. 2 Buchst. b) DS-GVO wegen verschiedener Verstöße gegen Vorschriften der DS-GVO erlassen.

Im Einzelnen haben wir zusammenfassend im Wesentlichen auf Basis der eigenen Einlassungen der Städte folgende Verstöße gegen Vorschriften der DS-GVO festgestellt:

- Es wurde gegen den Art. 5 Abs.1 Buchst. a) (Grundsatz der „Rechtmäßigkeit") i. V. m. §§ 4, 15 Landesdatenschutzgesetz bzw. Art. 6 Abs.1 Buchst. e) DS-GVO i. V. m. §§ 6 ff. baden-württembergisches Feuerwehrgesetz (FwG BW), im Fall von Gesundheitsdaten zusätzlich gegen § 15 Abs. 2 Landesdatenschutzgesetz bzw. Art. 9 Abs.1 DS-GVO sowie gegen Art. 5 Abs.1 Buchst. c) DS-GVO (Grundsatz der „Datenminimierung") verstoßen.

Eine Speicherung vollständiger arbeitsmedizinischer Bescheinigungen, vollständiger Personalakten sowie vollständiger Führerscheinkopien zum Zweck der Einsatz- und Personalplanung der Angehörigen der (Freiwilligen) Feuerwehr wäre bereits nach überwiegend eigener Einschätzung der Städte nicht bzw. nicht in diesem Umfang erforderlich gewesen. So war es etwa bei Führerscheinen nicht erforderlich, die kompletten Führerscheinunterlagen als Kopien zu speichern; es hätte vielmehr für den Zweck, die Fahrberechtigung der Angehörigen der Freiwilligen Feuerwehr zu kontrollieren, ausgereicht, die durchzuführende Sichtprüfung und den Kontrollzyklus zu protokollieren z. B. in Form von „Vorlage des Ausweises am…, Gültigkeit bis…, geprüft von…, Wiedervorlage/erneute Prüfung am…".

Nach einem solchen Datenleck zeigt sich, dass die Einhaltung des Grundsatzes der Datenminimierung nicht nur Selbstzweck ist, sondern darüber hinaus die betroffenen Personen vor einem hohen Risiko von Datenverlust und -missbrauch bis hin zu Identitätsdiebstahl schützt. Zudem muss man als verantwortliche stelle auch weniger Daten pflegen, was der Effizient dient.

Wir haben – zumeist übereinstimmend mit den Einlassungen der Städte – ebenfalls festgestellt, dass der Zweck für die Speicherung von Impfnachweisen, welche während der Corona-Pandemie aufgrund der sog. 3-G-Regel zulässig und erforderlich war, spätestens am 20. März 2022 mit dem Ablauf der Geltung der Vorschrift des § 28b Infektionsschutzgesetzes entfallen war und eine weitergehende Speicherung entsprechender Unterlagen in der Feuerwehr-Software nicht mehr zulässig und rechtmäßig war.

- Es wurde gegen Art. 5 Abs.1 Buchst. e) i. V. m. Art. 17 DS-GVO (Grundsatz der „Speicherbegrenzung") verstoßen.

In zwei Fällen mussten wir feststellen, dass kein etablierter, dokumentierter Löschprozess für die Akten der Angehörigen der Freiwilligen Feuerwehr existierte. Auch allgemeine Richtlinien zu Löschfristen lagen teilweise nicht vor.

Infokasten

Was ist eine URL?
URL = Abkürzung für uniform resource locator; eindeutige Webadresse einer Ressource (wie einer Webseite, einem Bild oder einer Datei) im Internet, die angibt, wie und wo sie gefunden wird, bestehend aus Protokoll (z. B. http://), Domain und Pfad, die direkt in den Browser eingegeben wird, um auf die Ressource zuzugreifen.

- Es wurde gegen die Pflicht zur Meldung einer Datenpanne nach Art. 33 Abs.1 DS-GVO verstoßen.

In einem Fall war eine Meldung nach Art. 33 Abs.1 DS-GVO trotz Kenntnis von der Betroffenheit erst nach sechs Monaten erfolgt, aufgrund von „Kommunikationsschwierigkeiten“ zwischen der externen Datenschutzbeauftragten und der Stadtverwaltung.

- Es wurde gegen die Benachrichtigungspflicht nach Art. 34 Abs.1 DS-GVO verstoßen.

In einem Fall wurden die von der Sicherheitslücke betroffenen Angehörigen der Freiwilligen Feuerwehr erst circa 8 Monate nach Kenntnis über den Sicherheitsvorfall und circa 2 Monate nach Kenntnis des Vorliegens eines hohen Risikos schriftlich über die Datenpanne informiert. Sie hätten nach Art. 34 Abs.1 DS-GVO hingegen unverzüglich benachrichtigt werden müssen.

Die betroffene Stadt hatte uns gegenüber eingeräumt, dass diese Prozessentscheidung nicht korrekt gewesen sei. Das lange Zuwarten mit der Benachrichtigung hatte sie damit gerechtfertigt, dass sie keine Hinweise auf einen tatsächlichen Zugriff bzw. Abfluss der Daten hatte und sie deshalb zunächst den Umfang des Sicherheitsvorfalls u.a. mithilfe eines sog. „Darknet-Scans“ klären wollte, um Fehlinformationen zu vermeiden. Die betroffene Stadt hat letztlich jedoch selbst eingeräumt, dass für die Erforderlichkeit der Benachrichtigung der von dem Sicherheitsvorfall betroffenen Personen nach Art. 34 DS-GVO maßgeblich ist, ob ein „voraussichtlich“ hohes Risiko besteht, nicht dagegen, ob ein tatsächlicher Zugriff bzw. Abfluss der Daten erfolgt ist.

- Es wurde gegen Art. 24 Abs. 1 i. V. m. Art. 5 Abs. 2 DS-GVO („Rechenschaftspflicht“) verstoßen.

In einem Fall wurde als Grund für eine um mehrere Monate verspätete Meldung nach Art. 33 Abs. 1 DS-GVO insbesondere eine fehlende spezifische Triage-Regel für behördliche Datenschutzschreiben im Posteingang bei der Stadtverwaltung angegeben. Wir haben zudem festgestellt, dass diese Stadt als für die Datenverarbeitung Verantwortliche gemäß Art. 4 Nummer 7 DS-GVO bereits ab dem Zeitpunkt, in dem sie von dem Sicherheitsvorfall erfahren hatte, die Pflicht gehabt hätte, ihre eigene Betroffenheit sowie das Ausmaß selbst zu überprüfen, was aber unterblieben war.

In einem weiteren Fall gab die betreffende Stadt an, dass unsere Rund-E-Mail vom 13. Dezember 2024 intern nicht an die zuständige Stelle weitergeleitet worden sei. Dadurch sei ihr erst mehr als 5 Monate später die eigene Betroffenheit von der Datenpanne bewusst geworden. Durch die nicht erfolgte interne Weiterleitung der o. g. E-Mail konnte diese Stadt uns gegenüber nicht in ausreichendem Maße nach Art. 5 Abs. 2 DS-GVO nachweisen, dass sie tatsächlich die nach Art. 24 Abs. 1 DS-GVO geeigneten technischen und organisatorischen Maßnahmen für eine verordnungsgemäße Verarbeitung umgesetzt hat. Sie hat somit gegen Art. 5 Abs. 2 DS-GVO („Rechenschaftspflicht“) verstoßen.

Die betreffende Stadt hätte mithilfe technisch-organisatorischer Maßnahmen, wozu auch die Ausgestaltung eines funktionierenden Postlauf- und Meldeprozesses gehört, dafür Sorge tragen müssen, dass ein Posteingang wie unsere E-Mail vom 13. Dezember 2024 als wichtige Mitteilung gefiltert und sodann wegen Fristlaufs unverzüglich dem für die weitere Bearbeitung zuständigen Mitarbeitenden weitergeleitet wird. Sie konnte damit den Nachweis, dass sie über die erforderlichen Eingangs-, Triage-, Weiterleitungs-, Bearbeitungs- und Meldeprozesse im relevanten Zeitraum verfügt hat, uns gegenüber nicht führen.

Aus den Erfahrungen im Rahmen unserer aufsichtsbehördlichen Tätigkeit rund um diesen Sicherheitsvorfall ziehen wir das Resümee, dass alle Städte und Gemeinden Baden-Württembergs – egal, ob und in welchem Maß sie von dem konkreten Sicherheitsvorfall betroffen waren – gut darin beraten sind, diesen Sicherheitsvorfall zum Anlass zu nehmen, ihren Umgang mit personenbezogenen Daten und den datenschutzrechtlichen Vorgaben und Anforderungen zu überprüfen: So ist es etwa ratsam, die Funktionsfähigkeit der internen Melde-, Triage- und Weiterleitungsprozesse bei einem Datenschutzvorfall zu überprüfen und sich im Fall der Einschaltung eines Auftragsverarbeiters zu vergewissern, dass zumindest eine Plausibilisierung der von diesem gelieferten Informationen möglich ist.

Zudem ist stets das Erfordernis zu hinterfragen, ob, wo und inwieweit vollständige Originaldokumente wie z. B. Führerscheine, Impfnachweise oder medizinische Tauglichkeitsnachweise abgespeichert werden dürfen. Geboten ist außerdem, bereits bei der Speicherung personenbezogener Daten eine systematische Löschroutine zu implementieren.

Wir regen in diesem Zusammenhang an, dass sich die Städte und Gemeinden untereinander, z. B. über das Feuerwehrausschuss-Gremium, austauschen, um eine einheitliche Fristenmatrix auszuarbeiten für die Dauer der Aufbewahrung verschiedener Unterlagen der Freiwilligen Feuerwehr. Dieser Vorfall zeigt, wie wichtig es ist, dass unnötige „Datenhalden“ und „Datenfriedhöfe“ erst gar nicht entstehen. Dies begrenzt in der Folge auch gleichzeitig das Ausmaß eines möglichen Sicherheitslecks und damit einhergehenden Risiken wie Identitätsdiebstahl z. B. bei Angriffen auf die IT-Infrastruktur.

Folgen Sie uns auf Mastodon und PeerTube

Aktuelles vom Datenschutz
und der Informationsfreiheit gibt es auf
den Social Media Kanälen des LfDI

mastodon

bawü.social/@lfdi
bawü.social/@lfdi_pressestelle

PeerTube

tube.bawü.social/a/lfdi_pressestelle

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Kapitel 6

Neues aus der Bußgeldstelle

6. Neues aus der Bußgeldstelle

Im vergangenen Jahr haben wir über 100 Bußgeldbescheide erlassen mit einer Gesamtsumme von mehr als 300.000 Euro. Wir empfehlen, die Rechte der Bürgerinnen und Bürger bestmöglich zu wahren.

6.1. Wirksam, verhältnismäßig, abschreckend

Wir haben im Jahr 2025 insgesamt 101 Bußgeldbescheide erlassen mit einer Gesamtsumme von 308.850 Euro. Im Jahr 2025 sind bei uns über 300 Neuverfahren eingegangen, womit der bisherige Höchstwert aus dem Jahr 2019 deutlich überschritten wird.

Nicht automatisch führt ein Bußgeldverfahren zu einem Bußgeld. Wenn wir Bußgelder erlassen, müssen diese in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Bei der Bemessung der Bußgeldhöhe ist beispielsweise zu beachten, welche Kategorien von personenbezogenen Daten betroffen sind, ob eine verantwortliche Stelle mit Vorsatz handelte, ob sie eigene Maßnahmen ergreift, um den Datenschutzverstoß zu minimieren und künftig möglichst auszuschließen, und ob sie kooperativ ist (s. Art 83 DS-GVO). Besonders sensibel sind zum Beispiel Gesundheitsdaten, Bankdaten oder Personalausweisdaten.

Zu den „Klassikern“ bei den Bußgeldern gehören nach wie vor die Bereiche der privaten Videoüberwachung, der Betrieb von Dashcams im Straßenverkehr, die Standortdatenermittlung mittels AirTags sowie Mitarbeiterexzesse in unterschiedlichen Varianten. Oftmals wurden nicht ausreichende technische und organisatorische Maßnahmen getroffen, was dann zu Datenschutzverstößen führte.

6.2. Wenn das Hautscreening beim Arzt zur Dauerüberwachung in der Dermatologie wird

Gegen die Betreiber einer großen Hautarztpraxis haben wir ein Bußgeldverfahren wegen eines vorsätzlichen Verstoßes gegen Art. 6 Abs.1 Buchst. f) DS-GVO und § 26 BDSG geführt – Grund war eine umfassende Videoüberwachung innerhalb der Praxisräume der Patient_innen und bediensteten Personen, die aus unserer Sicht nicht zuläsig war.

Der Vorfall wurde zur Anzeige gebracht. Der Vorwurf: In den Praxisräumen sind fünf Kameras angebracht, die (teilweise minderjährigen) Mitarbeitenden in Bild und Ton und auch Patient_innen in Behandlungsräumen aufzeichnet. Hinweise dazu sind nicht erkennbar angebracht worden. Gegenüber den Beschäftigten hat der Arbeitgeber argumentiert, dass die Videoüberwachung zur Prozessoptimierung und Effizienzsteigerung innerhalb der Praxis erforderlich sind. Eine Einwilligung der Mitarbeitenden sei auch nicht erforderlich, da die bloße Information ausreiche.

Wir haben uns vor Ort und mit einem richterlichen Durchsuchungsbeschluss in der Praxis ein eigenes Bild gemacht, die Polizei hat uns dabei unterstützt. Das Ergebnis: Konkret werfen wir den Betreibern der Arztpraxis vor, ohne Rechtsgrund mindestens im Zeitraum von Januar 2023 bis zum Tag der Durchsuchung mit insgesamt sieben Kameras sowohl den Praxisbereich mit den Arbeitsplätzen, den Empfangsbereich und auch

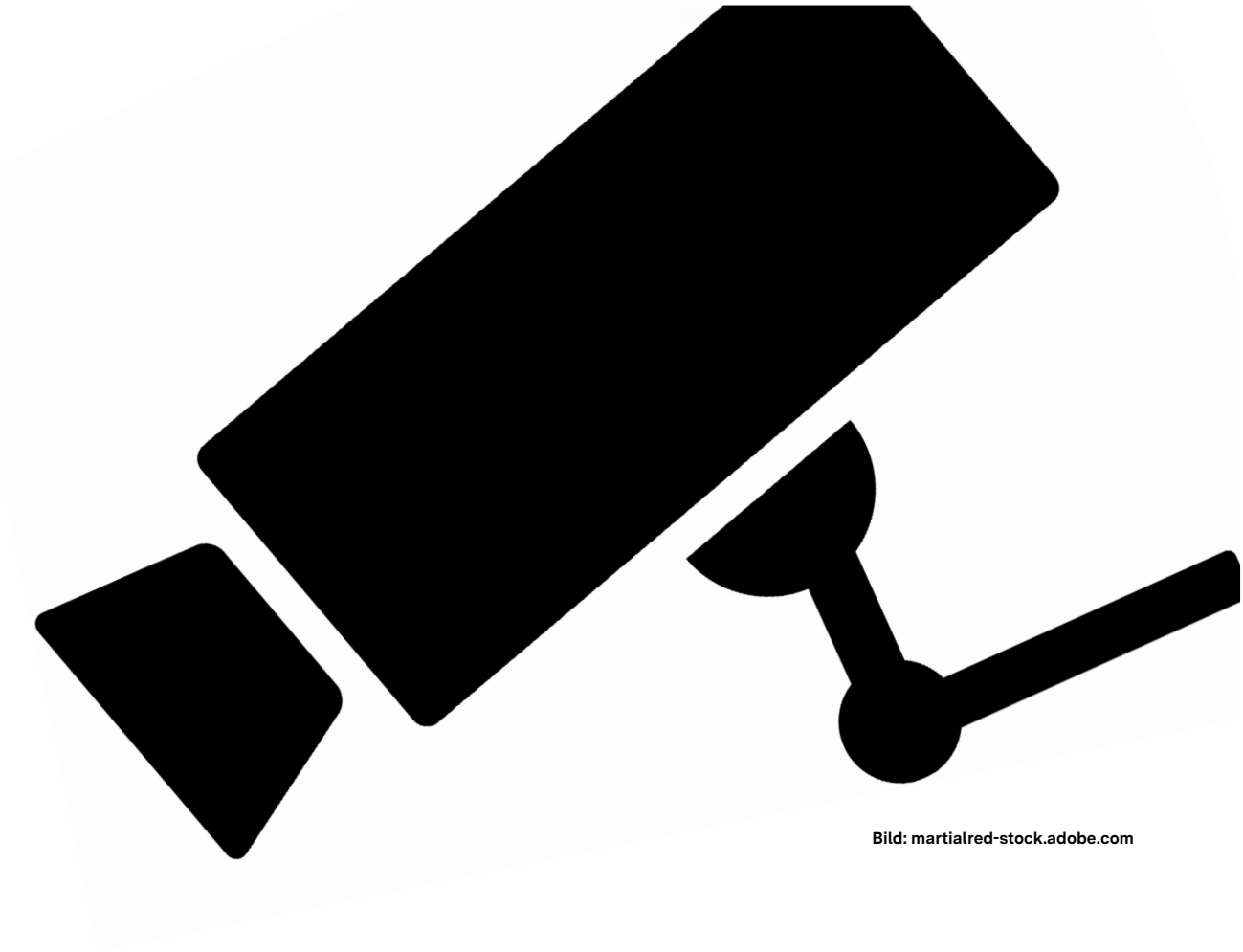


Bild: martialred-stock.adobe.com

teilweise Behandlungsräume im Live-Monitoring überwacht zu haben – in manchen Behandlungsräumen sind Patient_innen zur Behandlung weitgehend entkleidet. Die Kameras wurden demontiert und beschlagnahmt.

Wir haben festgestellt: Die Bildübertragung sämtlicher Kameras erfolgte auf einen zentralen Monitor im Thekenbereich. Dieser war je nach Standpunkt von Beschäftigten und aber auch Patient_innen einsehbar. Betroffen waren neben dem hohen Patienten_innenstamm insgesamt 24 Beschäftigte bei durchgehend starkem Patient_innenaufkommen.

Die Videoüberwachung in Praxisräumen ist eine komplexe Angelegenheit. Patient_innen müssen sorgfältig aufgeklärt werden und sich dazu verhalten können, und selbst mit einer solchen Information kann es kein Live-Monitoring geben, dass einem Public-Viewing gleicht. Hinzukommt: Eine rechtmäßige Einwilligung im Rahmen eines Beschäftigungsverhältnisses unterliegt hohen Hürden.

Sowohl die Überwachung von Patient_innen als auch der Beschäftigten ist somit sehr kritisch zu hinterfragen. Die Praxisbetreiber zeigen sich kooperativ. Dass Verantwortliche einsichtig sind, ist für uns sehr wichtig. Zugleich wirkt sich dies positiv für Verantwortliche in Bezug auf die Bußgeldhöhe aus. Wir gehen davon aus, dass wir das Verfahren zügig beenden können.

6.3. Rechtswidriger Einsatz von Dashcams

Verbraucher_innen werden heutzutage zu Billigpreisen in jedem Großmarkt und über Internetanbieter eine Vielzahl sog. Dash(board)cams angeboten. Mit diesen Kameras kann man dann den Straßenverkehr vom Fahrzeuginneren aus zu allen Seiten filmen – auch wenn das Fahrzeug beispielsweise dauerhaft beim Einkaufen geparkt wird.

Eine Speicherkarte von 512 GB garantiert, dass die Aufzeichnungen über mehrere Jahre erfolgen kann. Die Kameras ermöglichen heute auch Bildaufzeichnung in einer besseren Qualität als HD.

Zurückliegend hatten wir eine Vielzahl an Bußgeldverfahren im Bereich Dashcam, insbesondere seit sich die Polizei mit dieser Thematik verstärkt im Rahmen von Verkehrskontrollen befasst. Neben gemeinsamen Kontrollen mit der Polizei im Bereich der „Tuning-Szene“ und an gefahrengeneigten Rennstrecken für Motorräder, haben wir in diesem Jahr auch mehrere Schulungen durch die Bußgeldstelle organisiert. Etwa 1000 Polizeibeamt_innen haben an den Schulungen teilgenommen.

Nahezu immer wird bei den Ermittlungen festgestellt, dass über einen langen Zeitraum hinweg mittels der verbauten Kameras (Dashcam) dauerhaft und anlasslos der ruhende und fließende Straßenverkehr aufgezeichnet und die Daten dauerhaft auf der Speicherkarte verbleiben. Dies erstreckt sich neben den Bildaufzeichnungen auch auf die Anfertigung von Audioaufnahmen. Das bedeutet: Es wurden in unzulässiger Weise personenbezogene Daten verarbeitet. Diese Aufzeichnungen erfolgten oft aus mehreren Kameraeinstellungen – so wurden Fahrzeuge mit Kennzeichen sowie andere Verkehrsteilnehmer vor und hinter dem Fahrzeug aufgezeichnet.

So etwas kann teuer werden: Je nach Art und Dauer der Aufzeichnungen wurde zurückliegend gegenüber den Fahrzeughalter_innen bzw. den Fahrzugführer_innen ein Bußgeld in Höhe von 1000 bis 2000 Euro verhängt.

Obwohl uns das Thema Dashcams schon länger begleitet, soll an dieser Stelle noch einmal darauf hingewiesen werden, wie der Einsatz solcher Kameras rechtlich einzuordnen ist. Die Zulässigkeit des Verwendens einer Dashcam richtet sich nach Art. 6 Abs.1 Buchst. f) DS-GVO. Danach ist eine Videoaufzeichnung als spezielle Form der Datenverarbeitung nur zulässig, soweit diese nicht dauerhaft und anlasslos aufzeichnet. Die Aufzeichnungen müssen auch zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich sein und es dürfen keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die (versteckte) Beobachtung und Aufzeichnung von Straßenverkehrsteilnehmern in zumindest nicht geringem Umfang stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen dar. Dementsprechend ist eine permanente und anlasslose Aufzeichnung des gesamten Geschehens auf und entlang der Fahrstrecke zur Interessenwahrnehmung nicht erforderlich und damit in jedem Fall unzulässig.

Das nachvollziehbare Bedürfnis zum Betrieb einer Dashcam besteht gerade deshalb, da nahezu alle Verkehrsteilnehmenden im Schadensfall vertraglich verpflichtet sind, über ihre Kraftfahrzeug-Haftpflichtversicherung oder im Rahmen einer bestehenden Vollkaskoversicherung eine Selbstbeteiligung zu leisten. Diese Eigenbeteiligung betrifft sowohl Schäden am eigenen Fahrzeug bei einer Vollkaskoversicherung als auch mögliche Regressforderungen aus der Haftpflichtdeckung.

Ein zulässiger Einsatz der Kamera liegt aber ausschließlich dann vor, wenn erst im Falle eines Unfalls oder einer Gefahrenbremsung die Aufnahme mittels eines durch Unfallsensoren ausgelösten automatisierten Überschreibungsschutzes dauerhaft gespeichert werden. Hier handelt es sich aber auch nur um eine kurze Speicherdauer von 30 Sekunden. Dieser Zeitraum ist ausreichend, um einen Beweis zur Unfallverursachung führen zu können.

Ob ein Gerät technisch datenschutzkonform betrieben werden kann, ist daher vor der Inbetriebnahme zu prüfen. Können bestimmte Funktionen – etwa die Begrenzung der Aufzeichnung auf konkrete Anlässe oder eine automatische Löschroutine – nicht umgesetzt werden, ist der Einsatz der betreffenden Kamera zu unterlassen. Technische Mängel oder Herstellervorgaben heben die Pflichten des Verantwortlichen nicht auf. Dieser Umstand ist überaus bedauerlich, da uns bislang noch keine mobile Dashcam zur Prüfung vorlag, die datenschutzkonform betrieben werden kann. Ausführungen in der Betriebsanleitung zum datenschutzkonformen Betrieb sucht man leider oftmals vergeblich.

Actioncams: „Schau mal, wie ich mich mit dem Motorrad in die Kurve lege!“

Bei sogenannten Fun- und Actioncams an Zweirädern ist anzumerken, dass diese erst gar nicht für den Betrieb im öffentlichen Straßenverkehr bestimmt sind. Diese besondere Kamerasorte als Action und Fun-Produkt wurden von Herstellern für einen anderen Zweck als den Einsatz im öffentlichen Straßenverkehr konzipiert. So wird in einem Werbevideo eines Herstellers explizit auf den Outdoor-Einsatz unter Wasser beim Tauchen, Bergsteigen, Heliskiing, Downhill verwiesen.

In diesen Fällen stellt ein mehrstündiges Filmen im Dauerbetrieb dann auch kein Problem dar.

Technisch ist es bei diesen Kameras auch gar nicht möglich, die zeitliche Dauer auf eine anlassbezogene Aufzeichnung zu einem Unfallgeschehens oder einer Gefahrenbremsung zu begrenzen.

Diesen Umstand bemerken auch immer wieder Motorradfahrer_innen. Diese führen dann als Argument an, dass eine gefahrenfreie Bedienung des Geräts während der Fahrt nicht möglich ist, weshalb die Aufzeichnungen auch vor Fahrtantritt gestartet werde.

Eine Motorradfahrerin führte im Anhörungsverfahren zudem aus, dass diese sich bei der Bedienung während der Fahrt nicht ausreichend auf den Straßenverkehr konzentrieren könne. Auch wäre eine problemlose manuelle Bedienung zum An- und Ausschaltern der Kamera mit den gefütterten Motorradhandschuhen als übliche Ausstattung beim Motorradfahren überaus hinderlich. Wir glauben das unbedingt – und bei der Auswertung der Kamera durch unsere Bußgeldstelle konnte dieser Umstand auch deutlich auf mehreren Videos erkannt werden. Aber wie gesagt: Diese Kameras sind nicht fürs Motorradfahren geeignet.

In sämtliche zurückliegenden Verfahren zeichneten die Kameras auch den Ton auf. Deutlich wahrnehmbar waren daher durchaus auch mal Streitgespräche mit dem Ehepartner oder den Beteiligten nach einem Unfall, ausgesprochene Beleidigungen gegenüber anderen Verkehrsteilnehmenden oder abschließend dann meist das Gespräch mit der Polizei im Rahmen der Verkehrskontrolle vor der erfolgten Sicherstellung der Kamera. Als wir die Speicherkarten ausgewertet und dafür die abgelegten Dateien geöffnet haben, donnerte uns vor allem aber die Musik des Radios entgegen, es gab zeitweise auch Gesangseinlagen von Fahrzeugführer_innen. So amüsant das klingen mag – und jedem sei die eigene Gesangseinlage gegönnt und die ist auch datenschutzrechtlich nicht zu beanstanden – dauerhafte Ton- und Bildaufzeichnungen von anderen Verkehrsteilnehmenden sind schon eher kostspielige Angelegenheiten.

Tonaufzeichnungen im Taxi

Tonaufzeichnungen durch eine Dashcam können durchaus auch nützlich sein und einen erheblichen Beweiswert haben. Gleichfalls steht man aber unter Umständen mit dem Gesetz im Konflikt. Das bekam ein Taxi-Unternehmen zu spüren.

In einem Taxi erfolgte durch den Einzelunternehmer über einen langen Zeitraum eine anlasslose und dauerhafte Innenraumüberwachung mit einer Innenraum-Dashcam bei der nicht nur Bildaufnahmen, sondern auch Tonaufzeichnungen vorgenommen wurden. Diese Form der Überwachung betraf die Fahrgäste im Fahrzeug, sowie Passanten beim Ein- und Ausstieg, ohne dass diese Personen über die Aufnahme informiert wurden und ihre Einwilligung erklärt hätten. Die Kameraeinheit war so installiert, dass der Innenraum vollständig erfasst wurde.

Der Vorfall wurde durch geschädigten Kunden zur Anzeige gebracht, nachdem in einem Zivilverfahren der Rechtsanwalt Videosequenzen mit Ton als Beweismittel eingebracht hatte. Diese enthielten Gesprächsinhalte zur Höhe des verhandelten Fahrtpreises. Aufgrund der Kooperation mit unserer Behörde erging nur ein Bußgeld im mittleren vierstelligen Bereich gegen den Betreiber.

Infokasten

Fahrzeughalter_innen sind für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich, insbesondere wenn diese auch als Fahrzeugführer_innen die tatsächliche Gewalt über das Fahrzeug und deren Gerätschaften ausüben. Die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem Einsatz solcher Geräte liegt unstrittig beim jeweiligen Nutzenden (Art. 4 Nr. 7 DS-GVO).

6.4. Datenschutz im Bereich der Immobilienbranche

Zurückliegend mussten wir feststellen, dass es im Bereich der Maklerbranche in Sachen Datenschutz noch erheblichen Nachholbedarf gibt. Seit Inkrafttreten der DS-GVO im Mai 2018 scheint es, als hätten einige Maklerbüros lediglich standardisierte Datenschutzhinweise auf ihren Webseiten übernommen, ohne sich zuvor eine fachliche Beratung eingeholt zu haben.

Der „unentschlossene" Hausverkäufer

Ein Fall hat uns besonders beschäftigt: Offenbar hatte ein Makler lange nach einem Käufer für eine Immobilie gesucht, und als der Käufer endlich gefunden wurde, sprang der Verkäufer ab und wollte nicht mehr verkaufen. Er kündigte den Maklervertrag ohne Begründung. Provision adé? Nicht mit mir, dachte sich der Makler wohl.

Aus Angst, dass hier der Verkauf hinter dem Rücken des Maklers abgewickelt wird und dem Makler damit die Provision entgehen könnte, übersandte dieser dem abgesprungenen Verkäufer eine Liste mit einer hohen Anzahl von sogenannten „Kaufinteressenten" mit Vor- und Nachnamen, Wohnanschriften, sowie deren telefonische und elektronische Erreichbarkeit. Die Übermittlung erfolgte, nachdem sich der Verkäufer vom Maklervertrag „gelöst" hatte, einhergehend mit der Erklärung vom Verkauf seiner Immobilie Abstand nehmen zu wollen.

Ergänzend erfolgte durch den Makler noch der Hinweis auf die vertragliche Vereinbarung, dass ein fälliger Provisionsanspruch bestehen würde, sollte es nachträglich mit einem der genannten Personen auf der Liste zu einem späteren notariellen Kaufvertrag hinsichtlich der Immobilien kommen. Die Interessentenliste wurde mit einer Beschwerde bei unserer Behörde zur rechtlichen Bewertung und etwaiger Sanktionierung eingereicht.

Auch wenn es nicht wirklich überzeugend klingt, als Makler „sicherheitshalber" eine umfangreiche Namensliste einem potenziellen Verkäufer zu schicken, hat ein solches Verhalten zunächst eine mögliche Grundlage: Grundsätzlich kann nach der Rechtsprechung ein berechtigtes Interesse des Maklers an der Verarbeitung personenbezogener Daten bestehen, wenn dies erforderlich ist, um seinen Provisionsanspruch gemäß § 652 BGB durchzusetzen.

Doch ganz so einfach ist es dann doch nicht. Die Verarbeitung nach Art. 6 Abs.1 Buchst. f) DS-GVO setzt bei einem berechtigten Interesse auch eine umfassende Interessenabwägung voraus. Das Interesse des Maklers an der Geltendmachung des Provisionsanspruchs muss schwerer wiegen als das Recht der betroffenen Personen auf den Schutz ihrer Daten. Das bedeutet übersetzt: Für den Zweck angemessen wäre eine auf das notwendige Maß beschränkte Liste. Ausreichend wäre daher gewesen, lediglich den Namen und die Wohnanschrift zu übermitteln. Die Weitergabe einer Interessentenliste mit einer umfassenden Datenfülle war demnach unverhältnismäßig und stellte zumindest einen Verstoß gegen den Grundsatz der Datenminimierung i.S. Art. 5 Abs.1 Buchst. c) DS-GVO dar.

Aber lag ein wirksamer Provisionsanspruch überhaupt vor? Nach genauerer Betrachtung war ein wirksamer Provisionsanspruch nach unserer Bewertung noch gar nicht entstanden, da die erbrachten Leistungen des Maklers gegenüber den „Interessenten" noch nicht ausreichend dargelegt wurden.

Bei der Erstellung von Kundenlisten hat der Makler daher für das jeweilige Immobilienangebot eine klare Unterscheidung und Abgrenzung der einzelnen Interessentengruppen vorzunehmen. Hier fehlte es bereits an ausreichenden und nachvollziehbaren Differenzierungen und Abstufung der Interessenten als Käufer.

Zur Einordnung, was eine nachvollziehbare Differenzierung meint: Viele Interessenten lassen sich lediglich über aktuelle Angebote auf dem Wohnungs- und Immobilienmarkt informieren, ohne dass die Bereitstellung des vollständigen Exposés und der dazugehörigen Adressangabe und Angaben zum Verkäufer ergeht. Der nächste Schritt besteht dann darin, dass der Interessent aufgrund eines konkreten Kaufinteresses eine weitergehende Beratung durch den Makler erhält, insbesondere durch telefonische Abstimmungen oder die Übersendung eines vollständigen Exposés mit Adressangabe und Lage-/Aufteilungspläne). Anschließend wird in der Regel dann im Rahmen von einem oder mehreren Besichtigungsterminen ein konkretes Kaufinteresse nachgewiesen und es erfolgt beispielsweise eine Einsichtnahme in anonymisierte

Grundbuchauszüge oder ein konkretes Kaufpreisangebot wird abgegeben. Abschließend dann erfolgt das Ausfüllen des Datenblattes zur Vorbereitung des notariellen Kaufvertrages und die Übermittlung der Verkäuferdaten, sowie die vollumfängliche Einsicht in sämtliche Dokumente. Von der bloßen Interessenbekundung bis zum konkreten Preisangebot gibt es also unterschiedliche Wegmarken, Leistungen, die ein Makler erbringt.

Bei den auf der übersandten Liste des hier besprochenen Maklers handelte es sich aber gerade um aus dem gesamten Bundesgebiet aufgelisteten Personen, die ihre persönlichen Daten hinterließen, um in wiederkehrenden Abständen auf aktuelle Wohnungsangebote aufmerksam gemacht zu werden. Um einen begründeten Provisionsanspruch auszulösen, bedarf es aber – wie beschrieben, einer Mehrleistung des Maklers. In der Folge war die Sache ziemlich eindeutig: Die Übersendung der Gesamtliste erfolgte durch den Makler in unzulässiger Weise. Ein berechtigtes Interesse nach Art. 6 Abs.1 Buchst. f) DS-GVO in Verbindung mit § 652 BGB hat demnach auch nicht vorgelegen.

Der Makler ließ das gesamte Geschäftsmodell in der Folge auf Herz und Nieren durch einen Rechtsanwalt überprüfen. Diese Art der Mitwirkung wurde von uns bei der Bußgeldbemessung. Der Betroffene wurde dennoch mit einem hohen vierstelligen Betrag sanktioniert.

Nachhaltige Kundenbindung im Konflikt mit der Speicherzeitbegrenzung

Ein Beschwerdeführer meldete sich bei uns und teilte mit, dass er nach einer Gesamtdauer von 16 Jahren noch bei einem Makler auf der Kundenliste war, obwohl dieser ihm nur einmalig auf Anforderung ein Immobilienangebot übermittelt hatte. Nach vielen Jahren erhielt der „Altkunde“ unaufgefordert eine Werbemail mit einem Immobilienangebot auf dessen Mailadresse.

Wir haben uns den Sachverhalt angesehen. Die Ermittlungen zeigten, dass hier tatsächlich noch antiquierte Daten in Form einer damals vergebenen Kundennummer, Vorname, Nachname, Wohnanschrift und die Mailadresse im System des Maklers existierten.

Wie sich gezeigt hat, existierte innerhalb des Betriebes kein funktionierendes Datenlöschungskonzept, mithin wurde gemäß Art. 32 DS-GVO der Verpflichtung von technisch-organisatorischen Maßnahmen zur ordnungsgemäßen automatisierten Pflege der existierenden Kundendatei nicht nachgekommen. Nach Art. 5 Abs.1 Buchst. e) DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie dies für einen bestimmten Verarbeitungszweck erforderlich ist („Grundsatz der Speicherbegrenzung“).

Hat sich ein Kunde also ausschließlich für eine bestimmte Wohnung interessiert, so sind nach Absage des Interessenten bzw. nach dem vermittelten Verkauf oder Vermietung dieser Immobilie die Interessentendaten zumindest nach Verstreichen der gesetzlichen Verjährungsfristen zu löschen. Provisionsansprüche verjähren binnen drei Jahren (§ 195 BGB), beginnend mit dem Schluss des Jahres, in dem der Anspruch entstanden ist.

Auch bei einem allgemeinen Auftrag eines Interessenten zur Dauervermittlung einer Immobilie dürfen die Daten zwar fortlaufend gespeichert werden. Hier hat aber eine Routine für die Löschung von Interessentendaten oder ein Turnus für eine regelmäßige Überprüfung zu erfolgen, ob der Betroffene überhaupt noch Interesse an der Erfüllung des Vermittlungsauftrags hat. Ist der Betroffene an der Vermittlung nicht mehr interessiert, sind die Daten zu löschen. Die vorliegenden Datenspeicherung der Kundendaten über mehr als 15 Jahr war demnach unzulässig. Der Verantwortliche hat dann auch nachvollzogen, was wir ausgeführt haben, und hat kooperiert. Dies führte dazu, dass das Bußgeld erheblich gesenkt wurde.

Protokolle der letzten WEG-Versammlungen plötzlich im Internet

Nur noch in den wenigsten Fällen erfolgt eine Versendung eines ausgedruckten „Exposé“ für ein Immobilienangebot auf dem Postweg. Im Rahmen der Tätigkeit eines Immobilienmaklers werden die Angebote oftmals auf Immobilienplattformen eingestellt und es werden auch relevanten Dokumente, die der Verkäufer an den Makler übergeben hat, hochgeladen. Im hier besprochenen Fall wurden jedoch alle Dokumente durch einen Makler online gestellt, insbesondere auch solche, die „Internes“ zum Zusammenleben der Hausgemeinschaft und der Wohnungseigentümergemeinschaft beinhalteten. Das war, so viel sei hier schon verraten, keine gute Idee.

Bei den betreffenden Dokumenten handelte es sich um Protokolle der letzten Eigentümerversammlungen

mit namentlicher Erwähnung der Eigentümer. Bescheinigungsvorlagen beim Finanzamt, Wirtschaftspläne, Jahresendabrechnungen für Heizung, Warmwasser und Kaltwasser und vieles mehr. Es wurden unzulässiger Weise eine Vielzahl personenbezogener Daten von Mietern und Eigentümern auf der Verkaufsplattform offengelegt.

Wie sich im weiteren Verlauf gezeigt hat, lag der Fehler darin, dass die zuvor eingescannten und digitalisierten Dokumente innerhalb der Makler-Software im falschen Ordner abgelegt wurden, wodurch beim Hochladen auf die Internetplattform auch diese vertraulichen Dokumente erfasst wurden.

Bis der Fehler erkannt und die Dokumente wieder runtergenommen wurden, waren die Dokumente mit den personenbezogenen Daten für Besucher_innen der Internetplattform über mehrere Tage öffentlich zugänglich. Unstrittig wurden daher personenbezogene Daten der Eigentümergemeinschaft veröffentlicht, ohne über eine Rechtsgrundlage i.S. Art. 6 Abs.1 DS-GVO zu verfügen. Es bestand weder eine Einwilligung der betroffenen Personen noch eine anderweitige rechtliche Grundlage, die die Veröffentlichung der Daten gestattet hätte.

Auch wurde gegen den Grundsatz der Vertraulichkeit und Sicherheit verstoßen, der in Art. 5 Abs.1 Buchst. f) DS-GVO („Integrität und Vertraulichkeit“) festgelegt ist. Dieser verpflichtet Verantwortliche dazu, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Vertraulichkeit und Sicherheit der Datenverarbeitung zu gewährleisten. Für den Prozess des Einstellens von vertraulichen Dokumenten im richtigen Ordner war bislang kein ausreichender Kontrollmechanismus implementiert, um die Fehlbedienung der Makler-Software und die anschließende Veröffentlichung sensibler Daten zu verhindern. Der fahrlässige Verstoß wurde mit einem angemessenen Bußgeld im mittleren vierstelligen Bereich sanktioniert.

6.5. Vom Laster gefallen

Zurückliegend übergab uns die Polizei einen interessanten Fall. Ein aufmerksamer Bürger hatte bemerkt, dass ein Entsorgungsfahrzeug auf der Fahrt zum Entsorgungshof einen Teil seiner Papierladung aus dem Container auf der Fahrbahn verloren hatte. Dieses Entsorgungsunternehmen ist ausschließlich für die Entsorgung des normalen Papiermülls zuständig, nicht jedoch für die Datenmüllentsorgung und die Vernichtung von Unterlagen.

Die hinzugezogenen Polizeibeamten erkannten, dass es sich hier um Dokumente eines ortsansässigen Automobilhandlers handelt. Dieses überregional tätige Unternehmen vertreibt eine Vielzahl an hochwertigen Fahrzeugen von namhaften Herstellern, die von den potentiellen Kunden oftmals auch (nur) zur Probe gefahren werden. Für diese Fahrten werden von dem Unternehmen zur Sicherheit eine Kopie des Personalausweises und des Führerscheins des Entleihers, der Entleiherin, angefertigt, die nach Rückgabe des Fahrzeuges nach einiger Zeit entsorgt werden. Gleiches gilt auch für die Verträge zu den Probefahrten. Solche Unterlagen fielen nun vom Laster – und führten zu einem beträchtlichen Bußgeld.

Bei der Entsorgung der Unterlagen kam es zu einer rechtswidrigen Offenlegung der sensiblen personenbezogenen Daten. Die hausinterne Konzeption des Unternehmens sah bislang vor, dass am jeweiligen Arbeitsplatz zwei Behältnisse stehen, die zwischen Papiermüll und Datenmüll unterscheiden. Für die Entsorgung des Datenmülls waren ausschließlich die Mitarbeitenden zuständig, nicht jedoch das Reinigungsunternehmen. Der Datenmüll war an einem zentralen Dokumentenbehältnis zu entsorgen, was aber an diesem Tag nicht so erfolgte.

Nicht ermitteln ließ sich im Zuge des Verfahrens, wer die Verträge zu Probefahrten, Führerschein- und Personalausweiskopien der Kunden im üblichen Papiermüll deponierte. Festgestellt haben wir aber, dass das Automobilunternehmen eine nicht ausreichende und lückenhafte Zwischenlagerung des Datenmülls an den Arbeitsplätzen der jeweiligen Mitarbeitenden betrieben hat. Dies zeigte sich gerade daran, dass Kopien von Personalausweisen und Führerscheinen mit personenbezogenen Daten in offenen Müllbehältnissen an den jeweiligen Arbeitsplätzen zwischengelagert wurden. Die Verantwortung zur finalen Entsorgung in einem zentral gelegenen geschlossenen Datenmüllcontainer wurde auf den einzelnen Mitarbeitenden übertragen.

Das Bereitstellen eines Datenentsorgungscontainers an einer zentralen Örtlichkeit in der Firma und damit verbundenen langen Wegen für die Beschäftigten stellt keine ausreichende technisch-organisatorischen Maßnahme für ein großes Unternehmen i.S. Art. 32

DS-GVO dar. Wie sich hier gerade wieder gezeigt hat, besteht die konkrete Gefahr, dass Datenmüll offen in den Müllbehältnissen am jeweiligen Arbeitsplatz zwischengelagert wird. Es ändert dann auch nichts, dass eine klare Zuständigkeitsregelung zur Entsorgung betriebsintern existiert. Eine Sichtung des Datenmülls, eine Speicherung durch Abfotografieren oder Wegnahme konnte jederzeit vorgenommen werden.

Wir vertreten die Position, dass offensichtliche Lücken und daraus resultierende Gefahren für die Betroffenen sich mit vereinfachten organisatorischen Maßnahmen schließen lassen, mit einer Dienstanweisung zu Lasten der Beschäftigten lässt sich das nicht regeln. Die Tatsache, dass unbekannte Dritte die Vertragsunterlagen mit den Kopien von Ausweisen und Führerscheinen auf offener Straße auffanden, zeigt gerade die Gefahren dieser Regelungslücke. Durch die Offenlegung der Kundendaten im Rahmen der finalen Entsorgung über den üblichen Papiermüll hatte das Unternehmen in zumindest fahrlässiger Weise gegen Art. 5 Abs.1 Buchst. f) DS-GVO verstoßen. Auch das Verlieren der „Ware“ durch das Entsorgungsunternehmen, welches zur tatsächlichen Offenlegung gegenüber Dritten gesorgt hat, ist dem Unternehmen zuzurechnen, da derartige Pannen bei einer datenschutzrechtlich ungesicherten Entsorgung von handelsüblichem Papiermüll nie ganz auszuschließen ist.

Das Unternehmen ist unseren Ausführungen gefolgt und war kooperativ. Das Bußgeld wurde entsprechend reduziert und auf 120.000 Euro festgesetzt.

6.6. Mitarbeiterexzesse werden sanktioniert

Unsere Bußgeldstelle musste sich auch in diesem Jahr wieder mit einer Vielzahl von Fällen des Mitarbeiterexzesses auseinandersetzen. Anfang des Jahres 2025 schlossen wir ein Verfahren ab, welches dann auch gesellschaftlich viel diskutiert wurde. Ein Polizeibeamter musste wegen einer rechtswidrigen Datenabfrage ein hohes Bußgeld von 3500 Euro zahlen. Unsere Ermittlungen zeigten: Der Polizeibeamte handelte aus frauenfeindlichen Motiven.

Der junge Polizeibeamte musste das Bußgeld zahlen, weil er ohne dienstlichen Anlass eine unrechtmäßige Abfrage im Melderegister mit den Daten einer zuvor kontrollierten Frau durchführte. Ziel war es, das hinterlegte Lichtbild der Person einzusehen um sich danach im internen Kollegenkreis mit dieser „Trophäe“ zu brüsten. Die befremdliche Abfragepraxis erläuterte er dahingehend, dass er Frauen auf einer Schönheitsskala nach Punkten von 1 bis 10 bewertet und ab einem bestimmten Wert ein Lichtbild von der Person im Melderegister abruft. Dieses Verhalten zeigt nicht nur einen schwerwiegenden Datenschutzverstoß, sondern offenbart eine sexistische und frauenfeindliche Gesinnung, die mit den Grundwerten der Gleichberechtigung bei der Polizei Baden-Württemberg unvereinbar ist.

Polizeibeamte haben Zugang zu sehr sensiblen Daten von Bürger_innen, genießen ein hohes Vertrauen in der Bevölkerung. Sie müssen verantwortungsvoll mit den ihnen im Rechtsstaat zugewiesenen Durchsetzungsrechten umgehen. Polizeibeamte dürfen dienstliche Datenbanken nicht für private Zwecke nutzen.

Der Bemessung zur Bußgeldhöhe liegt jeweils eine Einzelfallprüfung zu Grunde. Hier fiel die Sanktionierung wegen der diskriminierenden Herabwürdigung verschärfend aus.

Erfahren wir von einer missbräuchlichen Nutzung von dienstlichen Datenbanken zu privaten Zwecken, sanktionieren wir dieses Fehlverhalten konsequent. Andere Bereiche stehen der Polizei in nichts nach. So wurden gleichfalls Verfahren gegen Mitarbeitende aus dem Jobcenter, Beschäftigte aus der Kommunalverwaltung, aber auch Bankkaufleute bei Kreditinstituten geführt. Diese hatten auch auf die jeweiligen Informations- und Auskunftssysteme rechtswidrig und aus einer privaten Motivationslage zugegriffen.

Kapitel 7

Zahlen

7. Zahlen

7.1. Statistische Übersicht

Zeitraum jeweils vom 1. Januar bis 31. Dezember

	2017	2018	2019	2020	2021	2022	2023	2024	2025
Beschwerden	3058	3902	3757	4782	4708	3796	3817	4034	7673
Kontrollen	55	13	111	31	10	33	71	54	33
Beratungen [1]	1786	4440	3842	3285	2206	1935	1682	1360	934
Anmeldungen Bildung- und Beratungszentrum BIDIB				785	2016	3255	3731	4470	3205
Datenpannen	121	900	2030	2321	3136	2747	2913	3559	4059
Bußgeldverfahren (eingeleitet)		138	233	174	136	213	185	243	314
Beteiligung an Gesetzgebungsverfahren [2]								92	142

[1] ohne telefonische Beratung

[2] Norm- und Gesetzgebungsverfahren sowie Verordnungen und Verwaltungsvorschriften (vgl. dazu auch Kap. 3., S. 30 ff.)

Herausgegeben von
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Prof. Dr. Tobias Keber
Heilbronner Straße 35, 70191 Stuttgart
Telefon: 0711/615541-0
www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
Mastodon: bawü.social/@lfdi
PeerTube: tube.bawü.social
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Redaktion: Prof. Dr. Tobias Keber,
Cagdas Karakurt, Simone Markovic, Feli Stary (alle Koordinierungs- und Pressestelle)
Gestaltung, Reinzeichnung, Barrierefreiheit: bodon, konzeption und gestaltung
Illustration Umschlag: Y. Dwiputri
Februar 2026