Landtag von Baden-Württemberg **Drucksache 17 / 6100**

17. Wahlperiode **31.1.2024**

Mitteilung

des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

39. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg für das Jahr 2023

Schreiben des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vom 31. Januar 2023, Az. 0557.6/3:

Anbei übersende ich Ihnen meinen 39. Tätigkeitsbericht für den Datenschutz.

Prof. Dr. Keber

Eingegangen: 31.1.2024 / Ausgegeben: 6.2.2024

Zukunft mit Datenschutz gestalten

Unsere Freiheiten:
Daten nützen – Daten schützen

Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Baden-Württemberg

Tätigkeitsbericht Datenschutz 2023

Herausgegeben von
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Prof. Dr. Tobias Keber
Lautenschlagerstraße 20, 70173 Stuttgart
Telefon: 0711/615541-0
Telefax: 0711/615541-15
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: Cagdas Karakurt, Simone Markovic, Feli Stary, Koordinierungs- und Pressestelle, LfDI
Gestaltung, Reinzeichnung, Barrierefreiheit: kwasibanane (Reinhardt Jacoby)

Januar 2024
Veröffentlicht als Landtags-Drucksache 17/6100

39. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2023

Inhalt

8

Prof. Dr. Tobias Keber

Vorwort

Das vergangene Jahr war für den LfDI BW ein Jahr der Konsolidierung, des Wandels und des Aufbruchs. Wie kann das sein, so mögen Sie sich fragen, schließt das eine doch das andere vermeintlich aus. Nach nun einem guten halben Jahr im Amt des Landesbeauftragten kann ich sagen: Es geht.

Als ich zum 1. Juli 2023 meine neue Tätigkeit antrat, kam ich in eine selbstbewusste oberste Landesbehörde, deren Mitarbeitende mich mit ihrer Fachexpertise und ihrem Engagement, sich mit neuen Herausforderungen für den Datenschutz auseinanderzusetzen, begeisterte. Ich erlebte eine Behörde, die die Zeit der Unsicherheit – die das Warten auf eine neue Behördenleitung unweigerlich mit sich bringt – produktiv nutzte und sich unter der Interimsleitung von Dr. Jan Wacke auf ihre Stärken besann, Bestehendes weiterführte und die Expertise des Datenschutzes in Baden-Württemberg ungebrochen hochhielt. Den Digitalgipfel 2023 nutzte die Behörde, um auf diesem Weg aktiv als Ansprechpartnerin auf die Wirtschaft zuzugehen, in einem Forschungsprojekt der Kinder- und Jugendhilfe unterstützte sie beratend das Universitätsklinikum Ulm und das Landratsamt Tübingen, und auch im Bereich der Mobilität führte der LfDI seine Beratung fort. Dies sind nur einige wenige von den Beispielen, die mir verdeutlichten, wie facettenreich und wichtig die Aufgaben des Hauses sind, das ich dankenswerterweise übernehmen würde. Ein Dank gilt an dieser Stelle meinem Leitenden Beamten Dr. Jan Wacke, der mir eine hochmotivierte und offene Landesbehörde übergab. Deshalb überraschte es mich auch nicht, dass ich im Juli auf einen „fahrenden Zug“ aufsprang, indem ich gleich zwei Wochen nach meinem Amtsantritt unter anderem mit dem Europa-Parlamentarier Axel Voss zur Zukunft des Datenschutzes im Kontext der KI-Verordnung diskutierte, die zweite KI-Woche des Hauses ebenso wie ein Kocheinsatz beim Gesundheitstag auf mich warteten, und ich zum ersten Mal der Frage gegenüberstand, welches Bußgeld beim Tracking eines Lebenspartners angemessen ist.

Nun liegen die ersten sieben Monate als Landesbeauftragter für den Datenschutz BW hinter mir. Ich kann ein erstes Resümee ziehen und auch einen Ausblick wagen. In Anbetracht der vielfältigen Aufgaben, der zunehmenden Herausforderungen im Bereich KI und der zahlreichen neuen europäischen Gesetzesakte befindet sich die Behörde einem steten Wandel unterworfen und kann diesen Aufgaben nur als eine lernende Organisation gerecht werden. Durch das starke Fundament und die gleiche Blickrichtung aller Beteiligten im Haus

ist das möglich: Wir wollen einen ausgewogenen Datenschutz, der Zukunftstechnologien mit „Privacy by Design“ möglich macht. Wir wollen einen wirksamen Datenschutz, der europäische Werte in Zeiten von KI sichert. Wir wollen einen verständlichen Datenschutz, der Menschen in den Mittelpunkt rückt. Hieran zeigt sich, dass nicht nur die Themen vielfältig sind, sondern auch die Mittel, die wir einsetzen müssen. In Anbetracht wachsender Anforderungen und Anwendungsgebiete müssen wir stärker systemisch beraten, um Unternehmen, genauso wie öffentliche Einrichtungen und jeden Einzelnen zu erreichen, zu sensibilisieren und zu befähigen, Datenschutz wirksam und situationsadäquat zu leben. Hierbei ist es ebenso wichtig, das Projekt „Datenschutz geht zur Schule“ mit Leben zu füllen, Bürger_innen zur „Langen Nacht der Museen“ ins Haus einzuladen, Schulungen für Kommunen im Bildungszentrum BIDIB anzubieten, als auch Ministerien bei Projekten wie der Bildungsplattform oder beim Forum Gesundheitsstandort Baden-Württemberg zielführend zu unterstützen oder Unternehmen im Bereich des Beschäftigtendatenschutzes oder zur Vermeidung von Datenpannen zu beraten.

Abschließend und auch im Vorwort schon ausblickend: Das Thema „Datenschutz und KI“ ist beim LfDI BW schon lange angekommen und wird bereits von den Mitarbeitenden abteilungsübergreifend vorangetrieben. So war es mir möglich, ein deutschland-, wenn nicht europaweit erstes Diskussionspapier zu „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ vorzulegen, das auch im europäischen Ausland wahrgenommen und diskutiert wird, weshalb jüngst auch eine englische Übersetzung erfolgte. Eine hybride Veranstaltung hierzu vor wenigen Tagen mit annähernd 400 Teilnehmenden belegt die Strahlkraft und Relevanz des Themas.

Nicht nur hieran zeigt sich: Wir müssen europäisch denken und uns gleichzeitig unserer regionalen Stärken besinnen. Wir müssen fachkundige Ansprechpartner im Bereich des Datenschutzes für KI-Anwendungen sein. Der enge Austausch mit Unternehmen ebenso wie die Beratung von Startups oder die Begleitung von KI-Anwendung in Behörden ist hier essentiell. Wir sind im Aufbruch begriffen, als Datenschutz-Kompetenzzentrum im Bereich KI Baden-Württemberg zu stärken und wichtige Impulse für Zukunftstechnologien zu setzen. Ein gutes Beispiel ist auch der Bereich der Gesundheitsdatennutzung, die uns auch weiterhin beschäftigen wird, und bei der wir im projektierten Austauschformat unter Federführung der Landesregierung bereits ein gutes und, wie ich meine, auch vorbildhaftes Stück weitergekommen sind im Sinne eines gemeinwohlorientierten, gemeinschaftlichen und zukunftsausgerichteten Prozesses.

An die Bedeutung der informationellen Selbstbestimmung im Kontext zunehmender Digitalisierung – und nun KI – hat uns im Besonderen auch noch einmal der 40. Geburtstag des „Volkzählungsurteils“ im vergangenen Dezember erinnert.

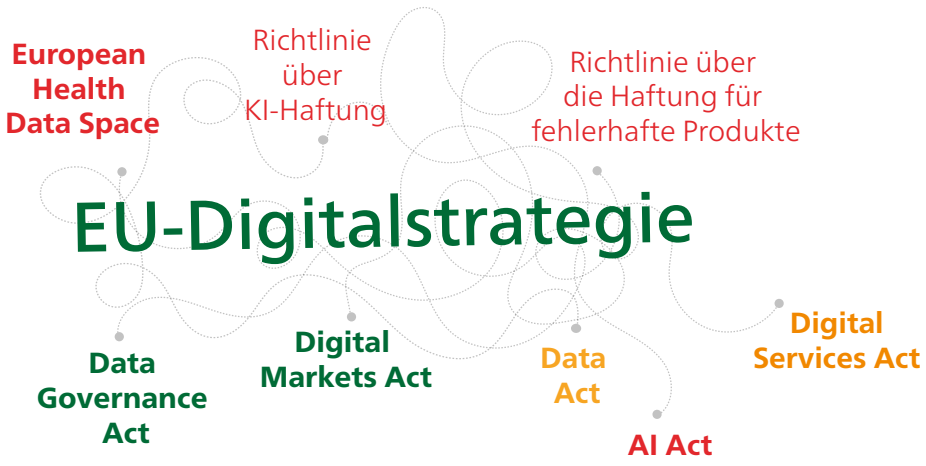
Ich bedanke mich bei der Landesregierung und den Abgeordneten des Landtags für das in mich gesetzte Vertrauen, sowie der Landesverwaltung und den Kommunen für die konstruktive Unterstützung und Stärkung meiner Behörde.

Ich freue mich auf die weitere Zusammenarbeit.

Ihr Landesbeauftragter

Prof. Dr. Tobias Keber

Vorwort



EU-Digitalstrategie

und weitere Informationen zu europäischen Regelungen zur Digitalisierung

commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_de

Data Governance Act (DGA)
seit 30. Mai 2022 anwendbar, eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R0868

Digital Markets Act (DMA)
seit 2. Mai 2023 anwendbar, eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R1925

Digital Services Act (DSA)
anwendbar (vollständig) ab 17. Februar 2024, in Teilen seit 16. November 2022
eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022R2065

Data Act
ab 12. September 2025 anwendbar
bmdv.bund.de/SharedDocs/DE/Anlage/DG/Digitales/eu-data-act-deutsche-fassung-22-12-23.pdf?__blob=publicationFile

AI Act (KI-VO)
Trilog, Verordnungstext in Verhandlung, vermutlich ab 2026 anwendbar
eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206

Richtlinie über KI-Haftung
Kommissionsvorschlag vom 28. September 2022, anwendbar ab: unklar
eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0496

Richtlinie über die Haftung für fehlerhafte Produkte
Kommissionsvorschlag vom 28. September 2022, anwendbar ab: unklar
eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0495&from=EN

European Health Data Space (EHDS)
Kommissionsvorschlag vom 3. Mai 2023, anwendbar ab: unklar
health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_de

Der LfDI in Europas digitaler Dekade

Der „digitale Wandel“ gehört zu den obersten Prioritäten der EU. Spürbar wird dies mit einer Vielzahl neuer Rechtssetzungsakte der EU-Kommission, welche auch die datenschutzrechtlichen Aufsichtsbehörden beschäftigt und vor die große Herausforderung stellt, die Schnittstellen der neuen Regelungen mit dem Datenschutzrecht zu identifizieren. Dabei stellen sich Zuständigkeits- und Verfahrensfragen, insbesondere wenn die Umsetzung von Regelungen den EU-Mitgliedstaaten eigenverantwortlich auf nationaler Ebene obliegt. Aber auch inhaltlich bieten die Regelungen Schnittstellen zum Datenschutzrecht, die es von den Aufsichtsbehörden zu beachten gilt. Insgesamt zeichnet sich damit ein völlig neues Aufgabenspektrum für uns ab.

The Digital Services Act package: DSA und DMA

Das Gesetz über digitale Dienste (Digital Services Act, kurz: DSA) und das Gesetz über digitale Märkte (Digital Markets Act, kurz: DMA) bilden ein einheitliches Regelwerk, das die folgenden Hauptziele hat:

- Schaffung eines sichereren digitalen Raums, in dem die Grundrechte aller Nutzenden digitaler Dienste geschützt werden;
- Schaffung gleicher Wettbewerbsbedingungen für die Förderung von Innovation, Wachstum und Wettbewerbsfähigkeit sowohl im europäischen Binnenmarkt als auch weltweit.

Der Digital Markets Act und die Taskforce Consumer&Competition

Der DMA ergänzt das Wettbewerbsrecht und soll das Verhalten bestimmter großer Digitalkonzerne, sogenannter „Torwächter“, regulieren. Torwächter sind große digitale Plattformen, die zentrale Plattformdienste anbieten und gewerblich Nutzende und Endnutzende in Verbindung bringen, z. B. Online-Suchmaschinen, App-Stores, Messenger-Dienste. Dabei spielen personenbezogene Daten eine wichtige Rolle – sind doch ganze Geschäftsmodelle „datengesteuert“. Es ist evident, dass die Rechtsrahmen für den Wettbewerb, den Datenschutz und auch den Verbraucherschutz nicht länger isoliert betrachtet werden können und die Aufsichtsbehörden fachübergreifend zusammenarbeiten müssen. Dies zeigte jüngst die EuGH-Entscheidung zu Meta gegen Bundeskartellamt (C-252/21).

In Artikel 40 des DMA wurde entsprechend eine „hochrangige Gruppe“ (High Level Group) aus fachübergreifenden Expert_innen, einschließlich dem Europäischen Datenschutzbeauftragten und dem Europäischem Datenschutzausschuss (EDSA), konstituiert.

Der EDSA hat infolgedessen im März 2023 eine Taskforce ins Leben gerufen, die sich dem Zusammenspiel von Datenschutz, Wettbewerb und Verbraucherschutz widmen soll. Das Hauptziel dieser „Taskforce Consumer&Competition“ besteht darin, die Verbindungen zwischen den verschiedenen einschlägigen Regelwerken zu klären und Synergien zu schaffen, um die Kooperation zwischen den verschiedentlich betroffenen Behörden zu stärken.

Für Deutschland engagieren sich neben uns auch Kolleg_innen vom Bund, aus Hamburg und Bayern in dieser Taskforce.

Der Digital Services Act, der Digitale-Dienste-Gesetz-Entwurf und die Social Media Expert Subgroup

Während der DMA in erster Linie für die großen Digitalkonzerne gilt, nimmt der DSA für die Durchsetzung des Grundrechts- und Verbraucherschutzes alle Vermittlungsdienste, Hosting-Dienstanbieter und Online-Plattformen in die Pflicht, indem er Regeln zu Sorgfaltspflichten und Haftungsausschlüssen enthält. Zu diesem Zweck müssen Diensteanbieter unter anderem Melde- und Abhilfeverfahren einrichten, die es Personen oder Einrichtungen ermöglichen, (potenziell) rechtswidrige Inhalte zu melden, und die Diensteanbieter müssen ent-

sprechend reagieren (notice-and-takedown). Nutzende, die häufig und offensichtlich rechtswidrige Inhalte bereitstellen, sind für einen angemessenen Zeitraum von der Nutzung des Dienstes auszuschließen.

Besonders bemerkenswert sind die Regelungen des DSA, dass Dienste nicht in einer Form angeboten werden dürfen, die Nutzende täuscht, manipuliert oder sonst in ihren Entscheidungen irreführt oder behindert ("Deciptive design patterns", täuschendes Design). Der EDSA hatte diesbezüglich bereits in seinen Leitlinien datenschutzrechtliche Anforderungen aufgestellt. Darüber hinaus besteht eine Kennzeichnungspflicht für Werbung auf Online-Plattformen, und es darf keine Werbung angezeigt werden, die auf der Profilbildung besonderer Kategorien personenbezogener Daten beruht (Art. 9 DS-GVO: Gesundheitsdaten, biometrische Daten, Religion, ethnische Herkunft usw.). Bei Minderjährigen darf Werbung niemals auf Profiling personenbezogener Daten beruhen. Dies sind nur einige beispielhafte und wenige Punkte, mit denen die Rechte von Verbraucher_innen durch den DSA gestärkt werden.

Die Social Media Expert Subgroup des EDSA wurde vom EDSA damit beauftragt, das Zusammenspiel des DSA mit der DS-GVO im Detail zu betrachten. Eine Arbeitsgruppe der Expert Subgroup wird hierzu eine Handreichung veröffentlichen. Wir sind aktiv an der Erstellung dieser Handreichung beteiligt.

☛ **Mehr zu irreführenden Designs:**

edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

DDG-E soll DSA in nationales deutsches Recht umsetzen

Bis Februar 2024 muss Deutschland gesetzlich festgelegt haben, wie es die EU-Vorgaben des DSA regelt. Seit Anfang August 2023 liegt ein entsprechender Entwurf für das Digitale-Dienste-Gesetz (DDG-E) vor, der die DSA-Bestimmungen in nationales deutsches Recht überführt. Der Referentenentwurf wurde vom Bundesministerium für Digitales und Verkehr (BMDV) verfasst. Zur Durchführung des DSA wird darin insbesondere die Bundesnetzagentur als zuständige nationale Koordinierungsstelle für die Beaufsichtigung der Anbieter von Vermittlungsdiensten und zur Durchsetzung des DSA benannt. Ende Dezember wurde der DDG-E im Bundeskabinett beschlossen.

In Bezug auf die Umsetzung der vielfältigen Rechtssetzungsakte der EU auf nationaler Ebene im Allgemeinen zeigt sich, dass eine – frühzeitige sowie stärkere – Einbindung und Beteiligung der Datenschutzaufsichtsbehörden beim „digitalen Wandel" der EU erforderlich ist. Die zahlreichen Schnittstellen der Rechtsakte mit dem Datenschutz müssen rechtzeitig identifiziert und betrachtet werden. Nur so lassen sich in Europas digitaler Dekade handlungsfähige Aufsichtsstrukturen schaffen.

Allein dieser Blick zeigt auf – wenn wir beraten und unterstützen wollen, müssen wir wissen, wie diese Regelungen und Strategien aussehen und wo Bezüge zur DS-GVO bestehen. Behörden und Unternehmen nehmen dankenswerterweise immer wieder unsere Unterstützung an. Es freut uns, dass unsere Stabsstelle Zuwachs durch eine neue Kollegin im Frühjahr 2023 erhalten hat. So wird es besser möglich sein, uns zusätzlich neuen Schwerpunkten und weiteren Themenfeldern in der europäischen Zusammenarbeit zu widmen und dieses Wissen für verantwortliche Stellen in Baden-Württemberg nutzbar zu machen.

Fazit: Globaler Blick, lokales Handeln

US Präsident Joe Biden hat Ende vergangenen Jahres eine Executive Order zur Regulierung von Künstlicher Intelligenz erlassen. Die G7-Staaten befassen sich mit Risiken von KI, im Bletchley Park in England haben sich zahlreiche Staaten und Unternehmen der Privatwirtschaft getroffen, um über den Einsatz von KI zu sprechen.

Informiert bleiben. Abonnieren Sie den LfDI-Newsletter. 👇

Die Europäische Union ist mit der Aushandlung und dem Ausbuchstabieren des Textes der KI-Verordnung auf der Zielgeraden. In Baden-Württemberg wollen öffentliche und nicht-öffentliche Stellen KI einsetzen oder setzen KI bereits ein.

☛ Mehr zu den Diskussionen über die KI-Regelung in den USA, im Zusammenhang mit G7 und Europa:

Der LfDI Podcast „Datenfreiheit" Folge 31:
tube.bawü.social/w/gNUJnCswmo2Rx1g7as6tDZ

Folge 33:
tube.bawü.social/w/3FSuLxqmVxxnDmEhHPttYT

Folge 34:
tube.bawü.social/w/bMsCWmWnYQU1dUiktGT1kV

Die KI-Verordnung ist nicht der einzige Rechtsakt, der für uns von Interesse ist. Wir müssen uns vermehrt mit europäischen Regelungen befassen, die das Digitalrecht betreffen und oftmals einen Bezug zum Datenschutzrecht haben. So müssen wir uns etwa mit DGA, DMA, DSA, EHDS und dem Data Act befassen. Diese Regelungen sind Teil der EU-Digitalstrategie. Hinzu kommen beispielsweise auch die KI-Haftungsrichtlinie und die Richtlinie zur Produkthaftung.

Neben der EU-Digitalstrategie stehen eine Digitalstrategie des Bundes sowie eine Datenstrategie. Zudem verfolgt der Bund eine KI- und eine Cybersicherheitsstrategie. Daneben und unabhängig davon verfolgt das Land Baden-Württemberg mit digital.LÄND eine eigene Digitalstrategie. Wir stehen inmitten dieses komplexen Mehrebenesystems von rechtlichen Regeln und strategischen Überlegungen.

Datenschutz koordinieren: Deutsche und Europäische Zusammenarbeit

Alle blicken nach Europa

Nachdem nach der Corona-Pandemie auch auf europäischer Ebene allmählich der Normalzustand eintritt, war 2023 wieder ein buntes und themenreiches Jahr in der Arbeit unserer Stabsstelle für Deutsche und Europäische Zusammenarbeit. Während im vergangenen Jahr die Arbeit an Projekten der Arbeitsgruppen des Europäischen Datenschutzausschusses (EDSA) oft noch in den digitalen oder jedenfalls hybriden Bereich verlagert waren, hat man 2023 erfreulicherweise wieder vermehrt auf Präsenz-Sitzungen gesetzt, um den so wichtigen persönlichen Austausch zwischen den europäischen Datenschutzaufsichtsbehörden zu ermöglichen. Während wir dies auch bei unseren hausinternen Schulungen zu aktuellen Entwicklungen aus allen Themenbereichen für unser Kollegium umsetzen und die Diskussionsrunden wieder mehr vor Ort stattfinden, bauen wir das Angebot an Online-Materialien für unsere Homepage dennoch weiterhin aus. Konkret haben uns in diesem Jahr wieder einige europäische Themen beschäftigt, von denen wir hier berichten möchten.

Streitbeilegungsverfahren

Auch im Berichtsjahr 2023 beschäftigten den EDSA zwei Streitbeilegungsverfahren im Sinne des Art. 65 DS-GVO. In diesen Verfahren trifft der EDSA einen verbindlichen Beschluss mit Bindungswirkung für die federführende Aufsichtsbehörde, wenn in einem grenzüberschreitenden Fall im Kooperationsverfahren hinsichtlich eines vorgelegten Beschlussentwurfs keine Einigkeit zwischen den betroffenen Aufsichtsbehörden und der federführenden erzielt werden konnte.

So nicht, Meta!

Eine spektakuläre Entscheidung traf der EDSA bereits im April im Zusammenhang mit Drittstaatentransfers (Kapitel V DS-GVO) durch den Konzern Meta Irland („Meta“). Die irische Aufsichtsbehörde DPC wurde darin verpflichtet, ihren vorgelegten Beschlussentwurf zu ändern und angesichts der Schwere des Verstoßes ein Bußgeld gegen Meta zu verhängen. Geahndet wurden die Übermittlungen personenbezogener Daten des Unternehmens in die USA auf der Grundlage von Standardvertragsklauseln (SCCs) im Nachgang des sogenannten „Schrems-II-Urteils“ des EuGH. Die DPC wurde außerdem angewiesen, Meta dazu zu verpflichten, innerhalb von sechs Monaten die Verarbeitung einschließlich der Speicherung der unrechtmäßig übermittelten personenbezogenen Daten von europäischen Nutzenden in die USA einzustellen. Mit 1,2 Milliarden Euro stellt das von der irischen Aufsichtsbehörde auf die Entscheidung des EDSA hin erlassene Bußgeld einen neuen Rekord auf.

☛ **Verbindlicher Beschluss 1/2023 zu dem von der irischen Aufsichtsbehörde vorgelegten Streitfall über die Datenübermittlung durch Meta Platforms Ireland Limited für ihren Facebook-Dienst (Artikel 65 DS-GVO):**

edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_de

Keine irreführenden Designs, bitte!

Für uns war der zweite verbindliche Beschluss des EDSA von besonderer Relevanz. Denn hierin setzten wir uns selbst erfolgreich für die Einhaltung der datenschutzrechtlichen Grundsätze bei der Gestaltung von Online-Plattformen ein. Aufgrund der Entscheidung des EDSA im August 2023 musste die irische Aufsichtsbehörde ein Bußgeld gegen das Unternehmen TikTok Technology Limited („TikTok“) in Höhe von 345 Millionen Euro verhängen. Zudem forderte der EDSA die irische Aufsicht auf, den Umgang mit sogenannten "Deciptive design patterns" auch unter dem Gesichtspunkt von Fairness und Treu und Glauben (Art. 5 Abs. 1 lit. a DS-GVO) besonders zu

betrachten und gegenüber dem Unternehmen die Unterlassung anzuordnen. Grund dafür war, dass das Unternehmen bei der Gestaltung der Optionen in Pop-Up-Fenstern durch "Deceptive design patterns" junge Menschen zu einem Verhalten verleitet hat, das sie tendenziell von datenschutzfreundlichen Einstellungen auf der Plattform abhielt.

Uns freut an diesem Ergebnis besonders, dass die Entscheidung des EDSA die Aussagen der europäischen Leitlinien zu "Deciptive design patterns" in sozialen Medien stärkt, die wir federführend erarbeitet haben. Das Verfahren macht deutlich, dass die Prinzipien von "data protection by design" und "data protection by default" nicht nur abstrakte Vorstellungen des Datenschutzes sind, sondern zeigt ihre konkreten praktischen Anwendungsfälle auf.

Gerade eine so gewichtige Entscheidung gegenüber einer großen Online-Plattform setzt ein wichtiges Zeichen gegen manipulative Einstellungen. Bald ist auch mit einer Übersetzung der Leitlinien zu Deceptive Design Patterns in sozialen Medien in die deutsche Sprache zu rechnen.

☛ Mehr Infos

Binding Decision 2/2023 on the dispute submitted by the Irish SA regarding TikTok Technology Limited (Art. 65 GDPR):

edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22023-dispute-submitted_de

Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them:

edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

Datenschutz durch Technikgestaltung statt Irreführen durch Design:

www.baden-wuerttemberg.datenschutz.de/datenschutz-durch-technikgestaltung-statt-irrefuehren-durch-design

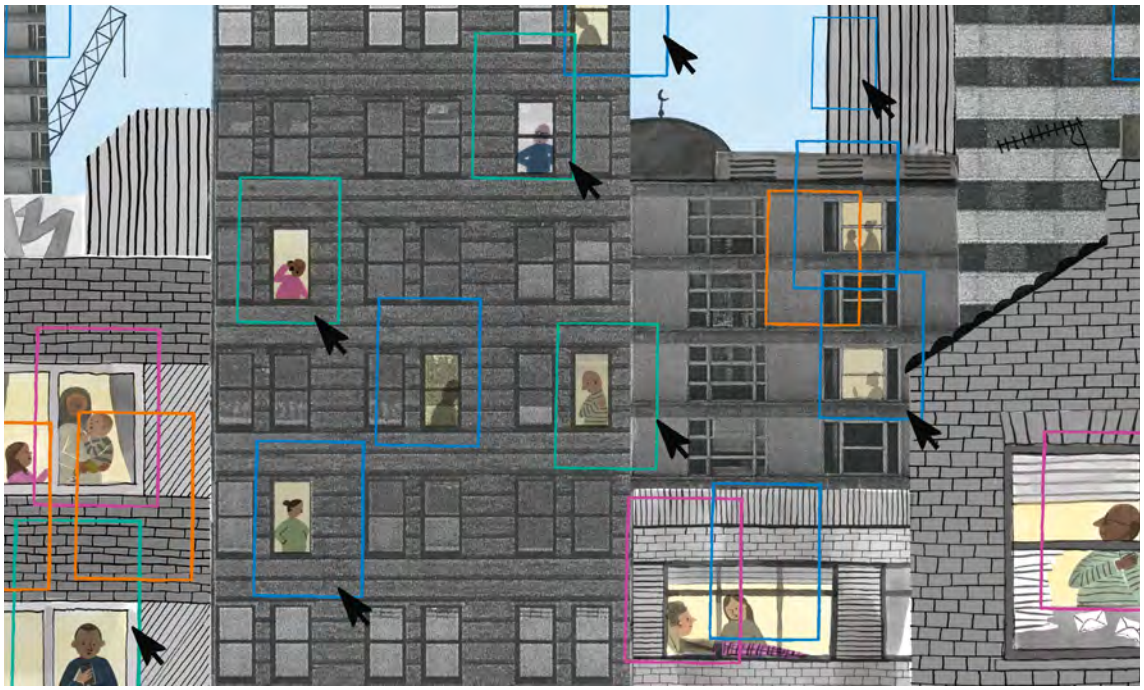


Bild: Emily Rand & LOTI / Better Images of AI / AI City / CC-BY 4.0

Smarte Häuser, smartes Leben, alles smart? Wirklich smart ist es, wenn Bürger_innen die Möglichkeit haben, souverän mit ihren personenbezogenen Daten umzugehen.

Beide Entscheidungen sind als historisch zu würdigen; nicht nur aufgrund der Höhe der verhängten Bußgelder, sondern auch als EU-weite Stärkung der Rechte von Nutzenden im Online-Umfeld. Es gilt also: Die europäische Zusammenarbeit wirkt – immer mehr!

Kooperation als Schlüssel zur Durchsetzungskraft

Nicht zuletzt der Name „Stabsstelle für Deutsche und Europäische Zusammenarbeit" – zeigt, wie wichtig die Kooperation der Datenschutz-Aufsichtsbehörden (geworden) ist. Wo Aufsichtsbehörden zusammenarbeiten, gemeinsam Hilfestellung geben, Problemfelder proaktiv sowie konstruktiv erkennen und behandeln oder zukünftige Entwicklungen begleiten, können sie gemeinsam mehr Kraft entfalten. So kann dem Datenschutz bei einem breiten Publikum Gehör verschafft werden, das seiner enormen Bedeutung Rechnung trägt. Und dies gilt sowohl im europäischen als auch im deutschen Kontext.

Die DS-GVO sieht ein Kooperationsverfahren zwischen den europäischen Aufsichtsbehörden explizit in den Artikeln 56ff. vor. Das schafft einen grenzüberschreitenden Austausch zwischen den Behörden der EU zu Einzelfällen, allgemeinen Rechtsfragen oder aktuellen Herausforderungen. Der EDSA gibt Raum für inhaltliche Diskussionen sowie formelle Abstimmungen, beispielsweise in den oben beschriebenen Streitbeilegungsverfahren. In dieses Geflecht auf Ebene der EU fügt sich die Zusammenarbeit der Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit ihrer jahrelangen Erfahrung ein.

Neben regelmäßigen Treffen der Hausleitungen und festen Sitzungen der DSK spiegeln auch ihre Arbeitskreise zu spezifischen datenschutzrechtlichen Themen auf Arbeitsebene die Struktur der europäischen Zusammenarbeit zwischen einzelnen Behörden und dem EDSA wider. Wir engagieren uns in beiden Bereichen vielseitig. Die Stabsstelle für Deutsche und Europäische Zusammenarbeit partizipiert in den europäischen Gremien in Form von formellen deutschen Vertretungspositionen oder durch die Mitarbeit an Leitlinien sowie anderen Veröffentlichungen des EDSA in den Expert_innengruppen.

Zudem ist die Stabsstelle in die Themen der Hausleitung rund um die DSK involviert. Wir unterstützen die DSK tatkräftig in ihren Arbeitsgruppen, um Stellungnahmen und Beschlüsse der DSK zu erarbeiten und für die finale Diskussion unter den Hausspitzen vorzubereiten. Gemeinsame Veranstaltungen der Aufsichtsbehörden der Länder und des Bundes sind Sinnbild der gemeinschaftlichen Ziele und Schwerpunkte der DSK und ermöglichen einen direkten Austausch, auch mit der Bürgerschaft. Die deutschen Datenschutzbehörden haben sich über die Jahre all diese Mechanismen erarbeitet, um schnelle und effektive Abstimmungen untereinander in der föderalen Struktur zu ermöglichen und auf nationaler wie europäischer Ebene Einfluss nehmen zu können.

Wie sich die deutschen Aufsichtsbehörden gegenseitig unterstützen und dass sie ein gut funktionierendes Kooperationssystem aufgebaut haben, verdeutlichen aktuell besonders zwei Papiere: Zum einen die Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder (DSK) zu den aktuellen Bestrebungen nach Änderung des Bundesdatenschutzgesetzes (BDSG) und zum anderen die Stellungnahme der DSK zum Entwurf der Europäischen Kommission zur Festlegung zusätzlicher Verfahrensregeln in grenzüberschreitenden Verfahren. Die gesetzgeberischen Vorhaben, die einheitliche und effektive Durchsetzung des Datenschutzes in Deutschland und Europa zu stärken, sind grundsätzlich zu begrüßen. Beide Stellungnahmen zeigen jedoch auf, dass eine Über-Formalisierung des Kooperationsverfahrens durch weitergehende Regelungen zusätzliche bürokratische Hürden aufbauen und die Zusammenarbeit zwischen den Behörden durch den erhöhten Aufwand sogar erschweren kann. Wie von der DSK ebenfalls ausdrücklich gefordert, sollte Ziel der Gesetzgebung vielmehr sein, die zwischen den Aufsichtsbehörden verabredeten praktikablen Vorgehensweisen und Modi aufzunehmen und durch eine

Institutionalisierung zu stärken. Die jahrelange Erfahrung und gewinnbringende Zusammenarbeit der Datenschutzaufsichtsbehörden kann damit verstetigt ihre Durchsetzungskraft national wie international gefestigt werden.

Stellungnahmen

Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder vom 6. September 2023 zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes mit Stand 9. August 2023:

www.datenschutzkonferenz-online.de/media/st/23_09_06_Laender_Stellungnahme_BDSG.pdf

Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 1. September 2023 zum Entwurf der Europäischen Kommission: Verordnung des Europäischen Parlaments und des Rates zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der Verordnung (EU) 2016/679 (COM(2023) 348 final:

www.datenschutzkonferenz-online.de/media/st/2023_09_01_DSK_Stellungnahme_KOM_E_VVO.pdf

Koordinierte Durchsetzungsmaßnahme zu Cloud-Diensten

Die koordinierte Durchsetzungsmaßnahme (Coordinated Enforcement Framework) des EDSA ist eine Schlüsselaktion seiner „Strategie 2021-2023" und soll die Durchsetzung des Datenschutzrechts stärken sowie die Zusammenarbeit zwischen den Aufsichtsbehörden intensivieren.

Die erste koordinierte Durchsetzungsmaßnahme des EDSA hatte die Nutzung von Cloud-Diensten durch den öffentlichen Sektor zum Inhalt. Bereits im Laufe des Jahres 2022 haben 22 Datenschutzbehörden im Europäischen Wirtschaftsraum (EWR) koordinierte Untersuchungen eingeleitet und insgesamt rund 100 öffentliche Stellen im EWR überprüft. Dabei ging es unter anderem um den Umgang mit Risiken für die Rechte und Freiheiten natürlicher Personen vor und während der Verarbeitung und insbesondere bei der Übermittlung personenbezogener Daten in Drittstaaten, die Verarbeitung von Telemetrie- oder Diagnosedaten durch eingesetzte Cloud-Dienstleister, die Vertragsgestaltung bei einer Auftragsverarbeitung und die Einbindung der behördlichen Datenschutzbeauftragten. Im Januar 2023 veröffentlichte der EDSA den Abschlussbericht dieser Prüfung und stellt darin die Ergebnisse der Untersuchung sowie die Kernelemente im Bereich der Nutzung von Cloud-Diensten durch den öffentlichen Sektor dar.

Wir haben uns an der Aktion beteiligt und den zentralen IT-Dienstleister des Landes Baden-Württemberg (BITBW) mit einem im EDSA abgestimmten Fragebogen angeschrieben und um Stellungnahme zu den eben genannten datenschutzrechtlichen Aspekten von Cloud-Diensten gebeten.

Aus datenschutzrechtlicher Sicht kann eine gut und professionell (extern) gemanagte Cloud grundsätzlich Vorteile haben, insbesondere dann, wenn das eigene Hosting ohne ausreichende personelle Kapazitäten erfolgen würde. Allerdings zeigt die europäische Auswertung der Ergebnisse, dass insbesondere zwischen großen Cloud-Dienstleistern und öffentlichen Stellen ein erhebliches Ungleichgewicht besteht und gegebenenfalls notwendige rechtliche und technische Anpassungen an Standardprodukte nur schwer umsetzbar sind.

Im Einzelnen zeigt der europäische Abschlussbericht, dass insbesondere folgende Punkte von den verantwortlichen Stellen beim Vertragsabschluss mit einem Cloud-Dienstleister beachtet und umgesetzt werden sollten:

- Prüfen, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss;
- Sicherstellen, dass die Rollen der beteiligten Parteien klar und eindeutig definiert sind;
- Sicherstellen, dass der Cloud-Dienstleister nur im Auftrag und gemäß den dokumentierten Anweisungen der öffentlichen Stelle handelt und dass jede mögliche Verarbeitung durch den Cloud-Dienstleister in eigener Verantwortung identifiziert wird;
- Sicherstellen, dass es eine wirksame Möglichkeit gibt, gegen neue Unterauftragsverarbeiter Widerspruch einzulegen;

- Sicherstellen, dass personenbezogene Daten in Bezug auf die Zwecke, für die sie verarbeitet werden, definiert werden;
- Die Beteiligung der behördlichen Datenschutzbeauftragten fördern;
- Zusammenarbeit mit anderen öffentlichen Stellen bei den Verhandlungen mit dem Cloud-Anbieter;
- Durchführung einer Überprüfung, um festzustellen, ob die Verarbeitung im Einklang mit der Datenschutz-Folgenabschätzung erfolgt;
- Sicherstellen, dass das Vergabeverfahren bereits alle notwendigen Anforderungen zur Einhaltung der DS-GVO enthält;
- Ermitteln, welche Übermittlungen im Rahmen der routinemäßigen Erbringung von Dienstleistungen erfolgen können und welche Verarbeitungen personenbezogener Daten für die eigenen Geschäftszwecke des Cloud-Dienstanbieters erfolgen, um sicherzustellen, dass die Bestimmungen aus der DS-GVO eingehalten werden, gegebenenfalls auch durch Ermittlung und Verabschiedung zusätzlicher Maßnahmen;
- Prüfen, ob die Rechtsvorschriften eines Drittlandes auf den Cloud-Dienstanbieter anwendbar sind und ob diese dazu führen würden, dass Anträge auf Zugang zu Daten, die der Cloud-Dienstanbieter in der EU gespeichert hat, nicht bearbeitet werden können;
- Sorgfältiges Prüfen des Vertrags und gegebenenfalls neu verhandeln;
- Überprüfen der Bedingungen, unter denen die öffentliche Einrichtung zu Überprüfungen und Kontrollen zugelassen ist und zu diesen beitragen kann, und sicherstellen, dass die Anforderungen aus Artikel 28 DS-GVO erfüllt werden können.

Wir werden die Ergebnisse der koordinierten Durchsetzungsmaßnahmen des EDSA auch in die eigene Praxis einfließen lassen und die Verantwortlichen und Datenschutzbeauftragten weiterhin beratend unterstützen.

☛ Mehr Infos

Der Bericht zur ersten koordinierten Durchsetzungsmaßnahme:
edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en

Die Pressemitteilung des EDSA:
edpb.europa.eu/news/news/2023/edpb-determines-privacy-recommendations-use-cloud-services-public-sector-adopts_en

Die Pressemitteilungen des LfDI:
www.baden-wuerttemberg.datenschutz.de/eu-weite-pruefung-cloud-dienste-oeffentlicher-bereich

www.baden-wuerttemberg.datenschutz.de/bericht-ueber-europaweit-erste-gemeinsame-datenschutzmassname

Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf

Hinweise des LfDI zur Nutzung von Microsoft 365 durch Schulen:
www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen

Die europäische Digitalwährung auf dem Weg in die nächste Phase: ein Rechtsrahmen für den Digitalen Euro

Zwei Jahre hatte die Europäische Zentralbank (EZB) abgewogen, ob sie den digitalen Euro einführen will. Basierend auf den Ergebnissen der „Untersuchungsphase für einen digitalen Euro“, die von Oktober 2020 bis zum Sommer 2023 dauerte, sollte entschieden werden, ob es möglich ist, eine europäische Digitalwährung einzuführen, die folgende Kriterien erfüllt: große Akzeptanz, kostenlose und einfache Nutzung, sofortige Abwicklung von Zahlungen, Verwendbarkeit für alle digitalen Zahlungen in der Eurozone sowohl für geschäftliche Zahlungen als auch direkt zwischen Personen, Möglichkeit einer Offline-Nutzung, größtmöglicher Schutz der Privatsphäre und Sicherheit. Der digitale Euro wäre eine elektronische Form von

Bargeld, das dieses nicht ersetzt, sondern ergänzt. Verbraucher_innen hätten die Möglichkeit, neben Banknoten und Münzen auch eine digitale Form von Zentralbankgeld kostenfrei zu nutzen, und dies umfassend und wenn nötig sekundenschnell. Immer im Blick hat die Europäische Zentralbank ihre Stellung im globalen digitalen Finanzwesen mit dem Ziel, eigene europaweite Zahlungstransferlösungen anzubieten, die Europa wettbewerbsfähiger und innovativer machen sollen, um dadurch die Abhängigkeit Europas von nichteuropäischen privaten Zahlungsdienstleistern zu verringern.

Diese Phase ist nun abschlossen: Im Juni 2023 legte die Europäische Kommission ihren Vorschlag für eine Verordnung zur Einführung des digitalen Euro vor (COM 2023/369). Die sogenannte „Vorbereitungsphase", die auf weitere zwei Jahre angelegt ist, startete im November 2023. In dieser Zeit sollen ein Vorschlag für einen verbindlichen Rechtsrahmen für die Einführung des digitalen Euro geschaffen sowie die Anbieter für die Entwicklung der Plattform und Infrastruktur ausgewählt werden.

In der gemeinsamen Stellungnahme vom Europäischen Datenschutzbeauftragten (EDSB) und vom EDSA wird die Gesetzesinitiative der Kommission grundsätzlich begrüßt. Allerdings wiederholt der EDSA seine Forderung vom Oktober 2021, dass die Grundsätze von „Privacy by Default and by Design" stärker berücksichtigt und in dem Vorschlag für einen Rechtsrahmen bei der Festlegung der technologischen Verfahren verbindlich vorgegeben werden müssen.

Zwar betont die EZB, dass das Eurosystem keinen Zugang zu Daten habe, die eine direkte Identifizierung der Endnutzer ermöglichen, oder diese speichere. Allerdings müsse der Schutz der Privatsphäre und der Datenschutz mit anderen politischen Zielen in Einklang gebracht werden: der Bekämpfung der Geldwäsche und der Finanzierung des Terrorismus sowie der Steuerhinterziehung.

Dies sehen der EDSB und der EDSA weiterhin als sehr kritisch und regelungsbedürftig an. Die Vorgaben zur Betrugsprävention müssten präziser gefasst werden. Zudem müsse gewährleistet werden, dass sämtliche Transfers zwischen der EZB und den nationalen Zentralbanken nur pseudonymisiert erfolgten. Dazu müsse der Gesetzgeber eine Verpflichtung erlassen, die dies verbindlich festlegt. Es sei insbesondere unklar, welche Aufgaben von der EZB als Aufsichtsbehörde selbst für die Betrugsbekämpfung und welche Aufgaben (und die damit verbundene Datenverarbeitung) von den Zahlungsverkehrsdienstleistern wahrgenommen werden würden. Daneben weisen beide auf die Anforderungen von Artikel 35 DS-GVO und Artikel 39 DS-GVO hin, eine Datenschutzfolgenabschätzung durchzuführen.

☛ Mehr Infos

A stocktake on the digital euro summary report on the investigation phase and outlook on the next phase, 18. Oktober 2023:
www.ecb.europa.eu/paym/digital_euro/investigation/profuse/shared/files/dedocs/ecb.dedocs231018.de.pdf

FAQ zum digitalen Euro:
www.ecb.europa.eu/paym/digital_euro/faqs/html/ecb.faq_digital_euro.de.html

Gemeinsame Stellungnahme vom Europäischen Datenschutzbeauftragten (EDSB) und EDSA: Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro:
edpb.europa.eu/system/files/2023-10/edpb_edps_jointopinion_022023_digitaleuro_en.pdf

Bild: lassedesignen-stock.adobe.com

KI als Raketentechnologie zu beschreiben ist einfach, aber wohin soll die Reise gehen? Die europäischen Regeln zeigen es auf. In diesen Regeln stecken die europäischen Werte.

Datenschutz und Künstliche Intelligenz

Derzeit steht die KI-Verordnung der Europäischen Union kurz davor, ausbuchstabiert zu sein. Darin wird wohl auch die Definition der OECD für KI als Grundlage genommen – wie präzise diese wiederum ist, mögen die Leser_innen selbst entscheiden:

Ein KI-System, so die Definition der OECD-Sachverständigengruppe für KI (AIGO), ist
» *ein maschinenbasiertes System, das für bestimmte von Menschen definierte Ziele Vorhersagen anstellen, Empfehlungen abgeben oder Entscheidungen treffen kann. Es nutzt maschinelle und/oder von Menschen generierte Inputs, um ein reales und/oder virtuelles Umfeld zu erfassen, davon ausgehend (automatisch, z. B. mithilfe von ML [Maschinelles Lernen], oder manuell) Modelle zu erstellen und mittels Modellinferenz Informations- oder Handlungsoptionen zu ermitteln. KI-Systeme können mit einem unterschiedlichen Grad an Autonomie ausgestattet sein.* «

☛ **Definition der OECD-Sachverständigengruppe für KI (AIGO):**

www.oecd-ilibrary.org/sites/6b89dea3-de/index.html?itemId=/content/publication/6b89dea3-de#section-d1e325

KI – von A wie Ach je, ein Atombombenvergleich, über P wie Prometheus bis Z wie Zentralisierung

Ob ein Vergleich mit dem nuklearen Vernichtungspotenzial einer Atombombe zutreffend und KI „jeder bisher geschaffenen Technologie überlegen ist" (KI wirkt atomar, FAZ 24. Mai 2023), wird sich noch zeigen. Das Potenzial der aktuell viel diskutierten generativen KI ist aber unbestreitbar beeindruckend.

Datenschutzrechtliche Anforderungen gelten für alle Verarbeitungen personenbezogener Daten und auch für KI gibt es keine Ausnahme hiervon. Da es sich insbesondere bei generativer KI mit einer Vielzahl von gekoppelten Verbindungen (Neuronen) um ein hochgradig komplexes und nichtlineares System handelt, kann systembedingt kaum erklärt werden, wie die KI zu ihrem Ergebnis kommt.

Dies führt bei einer KI-basierten Entscheidung gegenüber Bürger_innen dazu, dass nicht eindeutig die Gründe für diese Entscheidung dargestellt werden können. Wie der EuGH in seinem Urteil zur Verarbeitung von Fluggastdaten bereits 2022 feststellt, „kann es sich nämlich angesichts der für die Funktionsweise von Technologien der künstlichen Intelligenz kennzeichnenden mangelnden Nachvollziehbarkeit als unmöglich erweisen, den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat" (EuGH, vom 21. Juni 2022, Az. C-817/19 2022 Rn. 195; ähnlich auch das Urteil des District Court of Hague, Niederlande, C/09/550982 / HA ZA 18-388, 2020, zur Erkennung von Sozialhilfebetrug mittels einer KI-Anwendung).

Zumindest wenn eine Person durch KI einer Entscheidung unterworfen wird, „die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" (Art. 22 Abs. 1 DS-GVO), müssen geeignete Rechtsmittel zur Verfügung stehen, wie das Recht einer Person seitens des Verantwortlichen auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung (Art. 22 Abs. 3 DS-GVO). Um diese Entscheidung transparent darstellen zu können und damit nicht zuletzt auch ein Gericht die Entscheidung (be-)urteilen kann, müssen die Gründe für eine KI-Entscheidung außerdem nachvollziehbar sein. Die hochgradig komplexe und nichtlineare Beschaffenheit der aktuell diskutierten KI-Modelle hat zur Folge, dass die Transparenz und Nachvollziehbarkeit von KI-Anwendungen insoweit begrenzt ist, wie diese von Menschen verstanden werden kann.

Damit rückt das "P wie Prometheus" und das prometheische Gefälle, das die Diskrepanz „zwischen der Unvollkommenheit des Menschen und der immer größer werdenden Perfektion seiner Maschinen" bezeichnet (Von Menschen und Technik: Von der Apokalypse-Angst zur Euphorie, Tagesspiegel,

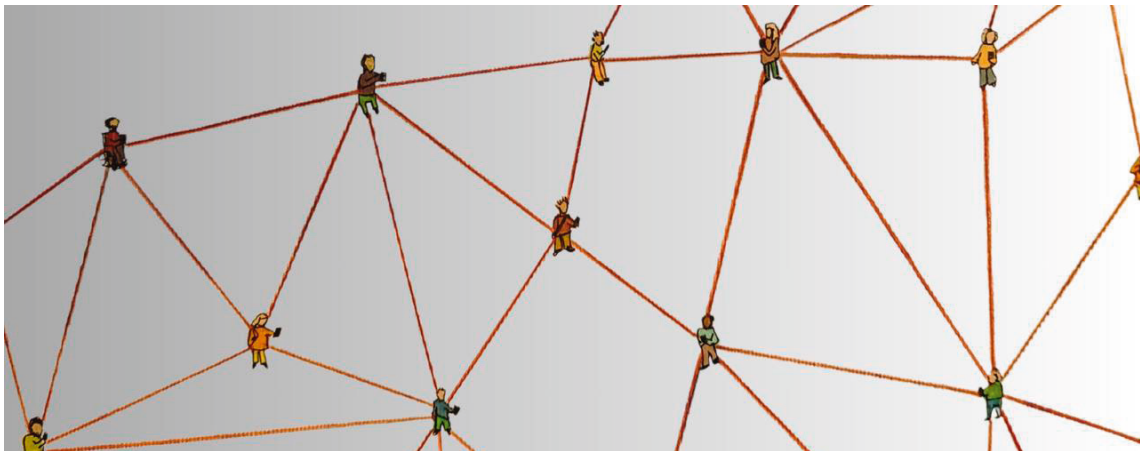


Bild: Jamillah Knowles & Reset.Tech Australia / © https://au.reset.tech/ / Better Images of AI / Detail from Connected People / CC-BY 4.0

Menschen sind oder werden miteinander verknüpft.

23. Februar 2001; dieser Artikel ist über 20 Jahre alt, die Auseinandersetzung mit dem Thema weiter aktuell), in den Vordergrund. Wieviel Transparenz und Nachvollziehbarkeit mit einer KI-Entscheidung einhergehen muss, kann letztlich nur gesamtgesellschaftlich bestimmt werden. Einschränkungen ergeben sich bereits jetzt mit Art. 22 DS-GVO und den mit dem Entwurf der KI-VO vorgesehenen verbotenen KI-Systemen. Gleichzeitig nennt der Entwurf der KI-VO bestimmte Verarbeitungen, die mit einem erheblichen öffentlichen Interesse einhergehen und damit zulässig sein sollen. Dazu zählen Verarbeitungen in den Bereichen der öffentlichen Sicherheit und öffentlichen Gesundheit, des Umweltschutzes und der Sicherheit und Widerstandsfähigkeit von Verkehrssystemen, kritischen Infrastrukturen und Netzen.

☛ Art. 22 DS-GVO: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

(1) Die betroffene Person hat das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(2) Abs. 1 gilt nicht, wenn die Entscheidung

a) für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist,

b) aufgrund von Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt, zulässig ist und diese Rechtsvorschriften angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten oder

c) mit ausdrücklicher Einwilligung der betroffenen Person erfolgt.

(3) In den in Abs. 2 Buchstaben a und c genannten Fällen trifft der Verantwortliche angemessene Maßnahmen, um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört.

(4) Entscheidungen nach Abs. 2 dürfen nicht auf besonderen Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 beruhen, sofern nicht Artikel 9 Abs. 2 Buchst. a oder g gilt und angemessene Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person getroffen wurden.

☛ Mehr Infos

Ist KI so gefährlich wie die Atombombe? FAZ, 24. Mai 2023:
www.faz.net/aktuell/feuilleton/debatten/ist-die-ki-von-openai-gefaehrlich-wie-die-atombombe-18916500.html

Von Menschen und Technik: Von der Apokalypse-Angst zur Euphorie, Tagesspiegel, 23.2.2001:
www.tagesspiegel.de/kultur/von-menschen-und-technik-von-der-apokalypse-angst-zur-euphorie-763861.html

„Lass mal das Innere eines Neuronalen Netzes ansehen!", Annika Rüll:
media.ccc.de/v/37c3-11784-lass_mal_das_innere_eines_neuronalen_netzes_ansehen

KI und Datenschutz, in BvD-NEWS, Fachmagazin für Datenschutzbeauftragte, 2/2023, S. 48–52:
www.bvdnet.de/wp-content/uploads/2023/07/32_BvD-399_News_2023-2_web.pdf

Im Dezember 2023 entschied der Europäische Gerichtshof in einer Frage die Datenverarbeitung der Schufa betreffen, dabei ging es auch um automatisierte Entscheidungen. Dieses Urteil hat Auswirkungen für den KI-Einsatz, davon ist auszugehen. Wir sprachen darüber in unserem Podcast Datenfreiheit ausführlich:
tube.bawü.social/w/bMsCWmWnYQU1dUiktGT1kV

"Z wie Zentralisierung" wird bei der Durchsetzung der DS-GVO im Zusammenhang mit KI und den Zuständigkeiten für die Materie insbesondere in Deutschland viel diskutiert und teils sogar ausdrücklich gefordert. Dabei ermöglicht gerade die föderale Struktur eine Nähe der einzelnen Behörden zu den verantwortlichen Stellen und eine intensive Beratung im Vorfeld der Verarbeitung. Der intensive Austausch zwischen den deutschen Aufsichtsbehörden sorgt für eine Verfestigung des Datenschutzrechts, organisiert über die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK).

Ein Jahr, das KI-Geschichte schrieb: Künstliche Intelligenz und ChatGPT

Mit seinem bereits im letzten Jahr veröffentlichten KI-Chatbot ChatGPT hat das Unternehmen OpenAI die Wahrnehmung von Bürger_innen auf KI neu geprägt. Auch wenn die Bewertung des Chatbots vom „plappernden Papagei" bis zur Schwelle der technologischen Singularität reicht, an der künstliche Intelligenz menschliche Intelligenz übertrifft, gilt es auch hier, bestehendes Datenschutzrecht umzusetzen. Und OpenAI muss den Aufsichtsbehörden die Fragen beantworten, die sie gestellt haben.

Am 30. März 2023 erließ die italienische Aufsichtsbehörde gegen OpenAI ein vorläufiges Verbot der Verarbeitung personenbezogener Daten von Betroffenen in Italien, da insbesondere keine ausreichende Transparenz über die Verarbeitung bestehe, eine Rechtsgrundlage für das Training des KI-Modells nicht erkennbar sei, die Korrektheit der verarbeiteten Daten nicht gewährleistet und der Jugendschutz nicht ausreichend sei. Diese Untersagung bescherte der datenschutzrechtlichen Diskussion um generative KI einen enormen Schwung. Die Datenschutzkonformität von ChatGPT wird nun sowohl auf europäischer als auch auf deutscher Ebene unter die Lupe genommen: Die Datenschutzaufsichtsbehörden der EU nehmen eine koordinierte Prüfung in der eigens dafür gegründeten Taskforce ChatGPT des Europäische Datenschutzausschuss (EDSA) vor, während die deutschen Aufsichtsbehörden in der DSK-Taskforce KI zu dem Thema zusammenarbeiten. Die Untersagung in Italien wurde, nach entsprechenden Nachbesserungen in den genannten Punkten durch OpenAI, beendet. Die Prüfung ist jedoch nicht abgeschlossen.

Die weitere Prüfung der europäischen wie deutschen Aufsichtsbehörden wird sich insbesondere darauf konzentrieren, wie bei der Verarbeitung personenbezogener Daten die Einhaltung der Grundsätze des Art. 5 DS-GVO, nämlich der Rechtmäßigkeit, der Zweckbindung, der Datenminimierung und Speicherbegrenzung sowie der Richtigkeit der Daten sichergestellt wird. Dabei sind sowohl die Da-

ten zu berücksichtigen, mit denen die Anwendung ursprünglich trainiert wurde, als auch die Daten, die die Nutzer_innen über sich und Dritte eingeben, sowie die personenbezogenen Daten, die durch ChatGPT generiert werden. Der Schutz Minderjähriger, der Schutz sensibler personenbezogener Daten und die Umsetzung der Betroffenenrechte müssen gegeben sein. Nicht zuletzt muss auch die datenschutzrechtliche Verantwortlichkeit geklärt werden, wenn Dritte den Dienst für ihre Zwecke nutzen. Um all dem näher auf den Grund zu gehen, unterstützen wir die Arbeit beider Taskforces.

☛ Mehr Infos

Künstliche Intelligenz : Der plappernde Papagei im Netz: www.tagesspiegel.de/kunstliche-intelligenz-der-plappernde-papagei-im-netz-9381044.html

Pressemitteilung: LfDI informiert sich bei OpenAI, wie ChatGPT datenschutzrechtlich funktioniert: www.baden-wuerttemberg.datenschutz.de/lfdi-informiert-sich-bei-openai-wie-chatgpt-datenschutzrechtlich-funktioniert

KI an der Schule

Über einen zunächst lockeren Kontakt zu Fortbildner_innen des Zentrums für Schulqualität und Lehrerbildung (ZSL) zum Thema KI an der Schule entstand eine intensivere datenschutzrechtliche Beratung für das Moodle-Modul fAIrchat, welches vom ZSL entwickelt wird. Dieses Modul, welches in Moodle eingebaut werden soll, wird als Vermittler zwischen Moodle-Nutzer_innen und ChatGPT eingesetzt, so dass keine Metadaten an den Betreiber OpenAI von chatGPT abfließen. Weiterhin werden durch die Nutzung des Application Interfaces (API) entsprechend den Vertragsbedingungen mit OpenAI (Terms of Use) diese Daten nicht zur Weiterentwicklung oder Verbesserung verwendet. Ebenso wird über die Nutzungsordnung von fAIrchat die Verwendung von personenbezogenen Daten untersagt, wobei die Lehrkraft auch nachträglich die Anfragen der Lernenden in Moodle nachlesen kann.

Sofern zusätzlich die jeweilige Lehrkraft die Schüler_innen auch ausdrücklich und für sie verständlich darüber aufklärt, dass sie keine personenbezogenen Daten in das System eingeben dürfen, und die Lehrkraft die Eingaben der Schüler_innen nachträglich überprüfen kann, die nachträgliche Kontrolle durch die Lehrkraft auch tatsächlich risikoangemessen zumindest stichprobenhaft erfolgt, scheint uns unter diesen Voraussetzungen eine Verwendung dieser KI im Rahmen des Unterrichts datenschutzrechtlich vertretbar.

KI-basierte Software in der ärztlichen Behandlung?

Eine radiologische Praxis wandte sich mit einer Beratungsanfrage über den datenschutzkonformen Einsatz von KI-basierter Software als Unterstützung für die medizinische Diagnostik an uns. Es handelte sich um eine Software, die ein Dienstanbieter über einen Auftragsverarbeitungsvertrag den radiologischen Arztpraxen zur Unterstützung in der Diagnostik bereitstellt.

Sobald Ärzt_innen KI-basierte Software in der Behandlung einsetzen, müssen sie sich in besonderem Maße mit der Software befassen, etwa damit, wie sie die Grundsätze der Verarbeitung personenbezogener Daten nach Artikel 5 Abs. 1 DS-GVO umsetzen. In unserer Beratung standen die Datenschutz-Folgenabschätzung nach Artikel 35 Abs. 1 DS-GVO über die KI-basierte Software und die Umsetzung der Grundsätze der Verarbeitung nach der DS-GVO im Vordergrund. Es stellten sich insbesondere folgende Fragen:

1. Setzt die verantwortliche Arztpraxis die KI-basierte Software über einen Auftragsverarbeitungsvertrag ein?

2. Wie setzt die verantwortliche Arztpraxis die Anforderungen an die Transparenz in den Informationspflichten nach Art. 12, 13 DS-GVO für die in der Behandlung eingesetzte KI-basierte Software um? Erklärt die verantwortliche Arztpraxis in den Datenschutz-Informationen den betroffenen Patient_innen die Funktionalität der KI-basierten Software?

3. Fand eine differenzierte Bewertung der Rechtsgrundlagen für den Einsatz der KI-basierten Software insbesondere hinsichtlich der erhobenen Trainingsdaten, der Verarbeitung für das Training der KI-basierten Software und den Einsatz der KI-basierten Software statt?

4. Verarbeitet die verantwortliche Arztpraxis bzw. der Auftragsverarbeiter die für den Einsatz der KI-basierten Software erhobenen personenbezogenen Daten für die Verbesserung des Modells weiter? Ist diese Weiterverarbeitung in den Informationen an die betroffenen Patient_innen aufgenommen und liegt dafür eine Rechtsgrundlage vor?

5. Hat die verantwortliche Arztpraxis die KI-basierte Software auf mögliche Auswirkungen auf die Rechte und Freiheiten natürlicher Personen im Rahmen der Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 DS-GVO mit den Besonderheiten des KI-Einsatzes bewertet und die technischen und organisatorischen Maßnahmen angepasst? Hierzu gehört, dass die Datenrichtigkeit bezüglich der Trainingsdaten z. B. in Gestalt der radiologischen Befunde und des trainierten Modells bewertet werden, was etwa die Kategorisierung, Aktualität, Repräsentativität und den von den Daten abgebildeten Wissensstand – also auch die Abwesenheit von verzerrenden Effekten (Bias) – betrifft. Schließlich hat sich die Bewertung auf die Qualität des von der KI-basierten Software generierten Ergebnisses im Hinblick auf potenzielle Schäden für die Individuen und Personengruppen zu erstrecken.

Sobald sich eine Arztpraxis entscheidet, gegebenenfalls über eine Auftragsverarbeitung KI-basierte Software bei der medizinischen Behandlung einzusetzen, bedarf es erklärender und leicht verständlicher Informationen über die Besonderheiten der Funktionalität im Sinne der Artikel 12 und 13 DS-GVO. Dazu gehören auch Informationen darüber, inwieweit die Ergebnisse der Software möglicherweise als Unterstützung einer optimierten und gegebenenfalls personalisierten ärztlichen Entscheidung dienen sollen. Entsprechend kann es besondere Dokumentationserfordernisse nach Art. 5 Abs. 2 DS-GVO für die jeweilige Entscheidung geben.

Als Rechtsgrundlage für den Einsatz von KI-basierter Software in der medizinischen Behandlung kommt einerseits Artikel 6 Abs. 1 Buchst. b in Verbindung mit Artikel 9 Abs. 2 Buchst. h DS-GVO mit dem Behandlungsvertrag im Sinne des § 630a des Bürgerlichen Gesetzbuches (BGB) und andererseits eine ausdrückliche Einwilligung nach Artikel 9 Abs. 2 Buchst. a DS-GVO in Betracht.

Die Rechtsgrundlage des Artikel 6 Abs. 1 Buchst. b in Verbindung mit Artikel 9 Abs. 2 Buchst. h DS-GVO mit dem Behandlungsvertrag nach § 630a BGB würde für diejenigen Konstellationen gelten, in denen der Einsatz von KI-basierter Software für die medizinische Behandlung zu den Haupt- oder Nebenpflichten des Behandlungsvertrages gehört. Allerdings dürfte der Einsatz von KI-Systemen für Diagnose- oder Behandlungszwecke derzeit (noch) nicht generell zum üblichen Stand der ärztlichen Kunst gehören, so dass eine derartige Verwendung solcher Systeme zumindest nicht ohne Weiteres von einem ärztlichen Behandlungsvertrag umfasst sein dürfte. Jedenfalls dann aber, wenn die Daten der Patientin oder des Patienten von der KI auch zur Verbesserung des genutzten KI-Systems verwendet werden sollen, dürfte der Bereich des für die Behandlung (der konkret behandelten Person) Erforderlichen verlassen werden, so dass die Verarbeitung zu dem Zweck der KI-Optimierung nicht mehr von dem Behandlungsvertrag gedeckt sein dürfte. Auch würde sich regelmäßig eine Weiterverarbeitung der personenbezogenen Daten durch den Anbieter der KI zur Verbesserung des Systems nicht mit einem Auftragsdatenverarbeitungsvertrag adressieren lassen. Soweit somit die personenbezogenen Daten der Patient_innen auch zur Verbesserung des in der Versorgung verwendeten KI-Systems verarbeitet werden sollen, dürfte daher stets eine hierauf bezogene ausdrückliche Einwilligung nach Artikel 9 Abs. 2 Buchst. a DS-GVO erforderlich sein. Dabei steht die behandelnde und die KI einsetzende Person unter anderem vor der Herausforderung, die behandelte Person trotz der vielfach kaum nachvollzieh- und antizipierbaren Funktionsweise einer KI-basierten Software hinrei-

chend über die mittels der Einwilligung zu legitimierenden Datenverarbeitungen zu informieren.

In den technischen und organisatorischen Maßnahmen haben die verantwortlichen Arztpraxen die hohen Schutz- und Vertrauensanforderungen nach Art. 25, 32 DS-GVO umzusetzen, was die Verschlüsselung, Pseudonymisierung und Anonymisierung der Daten durch die Auftragsverarbeiter voraussetzt. Ferner sind Verfahren notwendig, mit denen die verantwortlichen Arztpraxen und Auftragsverarbeiter eine Überwachung und eventuelle Fehlerbehebung der Software im Rahmen ihres Einsatzes umsetzen.

Und nicht zuletzt sind bei dem Einsatz eines KI-Systems in der Gesundheitsversorgung auch die Anforderungen aus Art. 22 DS-GVO einzuhalten: Nach Art. 22 Abs. 1 DS-GVO hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Bei der Entscheidung über eine Heilbehandlung dürfte die Voraussetzung, dass sie potenziell erheblich beeinträchtigende Wirkung entfalten kann, in aller Regel gegeben sein. Dann darf aber nach der genannten Norm grundsätzlich nicht die Maschine selbst die Entscheidung treffen, sondern die Entscheidung muss letztlich immer die behandelnde Ärztin – der behandelnde Arzt fällen. Damit die behandelnde Person aber die ihr obliegende Entscheidung überhaupt hinreichend substantiiert treffen kann, muss die KI ein Mindestmaß an Erklärbarkeit aufweisen. Andernfalls bestünde für die behandelnde Person die Gefahr, dass sie den Diagnose- bzw. Behandlungsvorschlag der KI kaum überprüfen könnte und deswegen – jedenfalls wenn sich der Einsatz von KI im Bereich der Gesundheitsversorgung durchsetzt und zum Standard wird – schon aus Gründen der Haftungsvermeidung angehalten wäre, der KI-Empfehlung mehr oder weniger unkritisch zu folgen.

Hilfreich für alle: Unser KI-Diskussionspapier

Die Verordnung der Europäischen Union zur Regulierung des Einsatzes von Künstlicher Intelligenz („KI-Verordnung“) befindet sich in ihrer Fertigstellung – Behörden, Unternehmen und weitere Institutionen prüfen jedoch bereits jetzt den Einsatz von KI oder nutzen bereits KI-Tools. Daher bedarf es auch jetzt datenschutzrechtlicher Hinweise, auf welchen Rechtsgrundlagen der Einsatz von KI gestützt werden kann, um nachhaltige digitale Entwicklung zu fördern, bei der Datenschutz und Künstliche Intelligenz von Anfang an gemeinsam gedacht werden. Wir sahen den wachsenden und drängenden Bedarf öffentlicher und nicht-öffentlicher Stellen, Hilfestellung im Bereich des datenschutzkonformen Einsatzes von KI zu erhalten, der nicht warten kann, bis die KI-Verordnung ausbuchstabiert ist.

Mit Blick darauf, dass das Datenschutzrecht von der KI-Verordnung unberührt bleibt und weiterhin gilt, beschritten wir einen neuen Weg. Wir verfassten ein Diskussionspapier zu „Rechtsgrundlagen im Datenschutz beim Einsatz von KI“, das eine erste Orientierung für öffentliche und nicht-öffentliche Stellen anbietet. Hierin steht die Frage im Mittelpunkt, wann und wie personenbezogene Daten für das Training und die Anwendung von Künstlicher Intelligenz verarbeitet werden dürfen.

Nicht nur, dass hiermit eine erste Einschätzung der Rechtssicherheit gegeben wird und direkt angewandt werden kann – uns ist auch bewusst, dass das Papier fortentwickelt werden muss. Auch wenn es uns als Landesbehörde schwergefallen ist, ein vermeintlich „nicht fertiges“ Papier zur Verfügung zu stellen, das nicht erst unzählige Runden durch Fachkreise gezogen hat, um jede Eventualität und Auslegungsspielräume berücksichtigt zu haben: Die Aktualität und die hohe Geschwindigkeit, mit der das Thema sich entwickelt, machen es nötig, auf seine eigene Expertise zu vertrauen und wegweisend voranzugehen, sich der Diskussion zu stellen, auch wenn man selbst noch der Herausforderung gegenübersteht, sich weiter orientieren zu müssen.

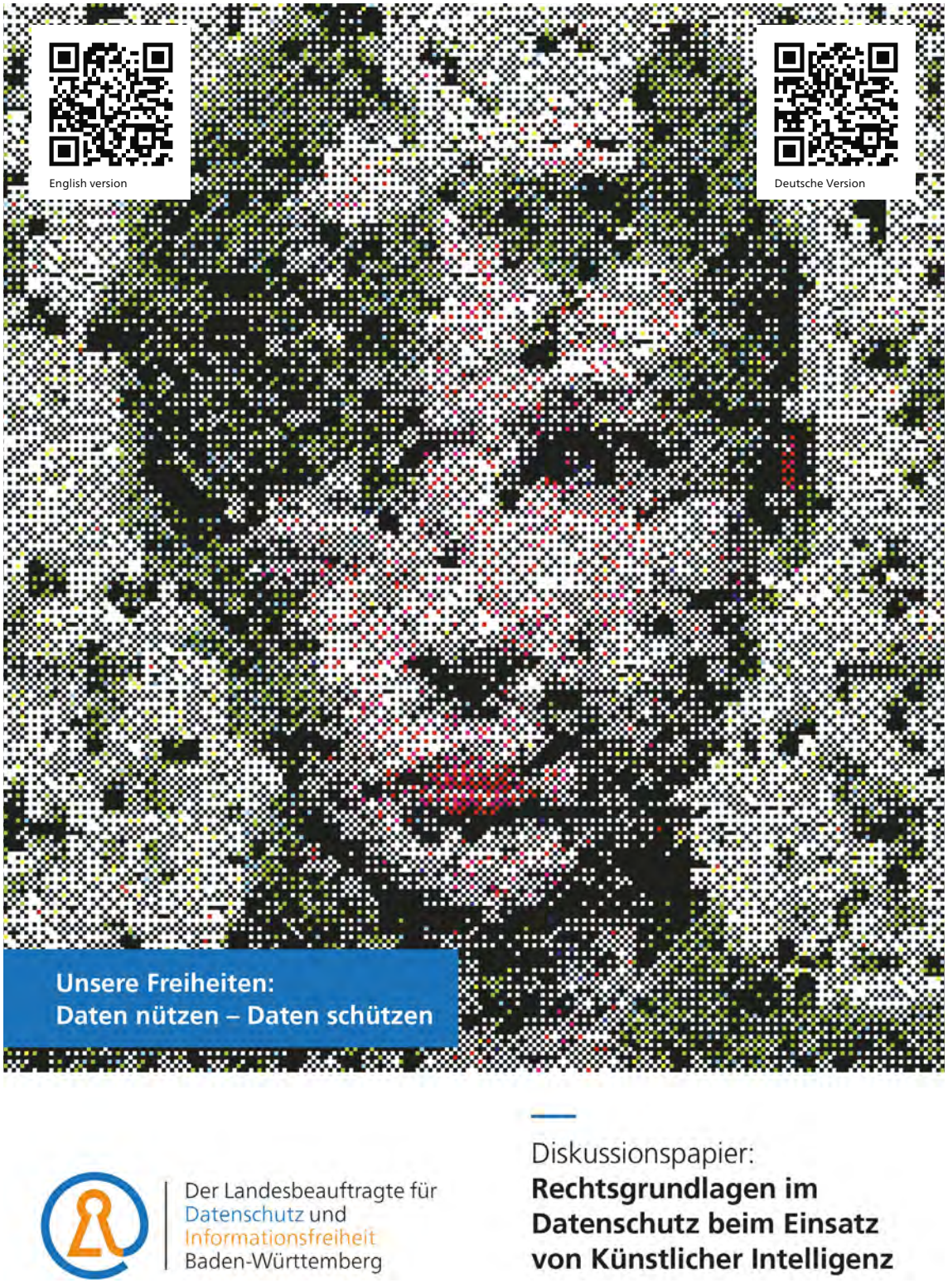


Bild: Local doctor-stock.adobe.com

Verantwortliche Stellen planen den Einsatz von KI und setzen KI bereits ein. Mit dem LfDI-Diskussionspapier liegt eine Arbeitshilfe vor, um Datenschutz und KI zusammenzubringen.

Bild: LfDI BW

Daniel Maslewski, KI-Beauftragter des LfDI für die Privatwirtschaft, und der Leiter der Abteilung Privatwirtschaft David Schweizer beim LfDI sprachen beim Digitalgipfel darüber, wie Datenschutz das Vertrauen in digitale Anwendungen stärkt.

Erstmalig hat eine Landesdatenschutzbehörde ein derartiges Arbeitspapier als erste rechtliche Einschätzung bereitgestellt – mit der Option, „sich eines Besseren belehren zu lassen". So haben wir das Papier zur Kommentierung auf unserer Homepage zur Verfügung gestellt (bis 1. Februar 2024) und innerhalb einer hybriden Veranstaltung mit bis zu 400 Interessierten diskutiert. Neben der Erkenntnis, dass unser Livestream bei über 330 Online-Teilnehmenden „in die Knie" gezwungen wird, zeigte das immense Interesse von Vertreter_innen aus Ministerien, anderen Behörden, Unternehmen, öffentlichen Einrichtungen und auch anderen LfDIs, dass wir das richtige Gespür hatten, welch immenser Bedarf besteht. Selbst im Ausland behalf man sich in Fachkreisen mit Übersetzungsprogrammen, um die Handreichung diskutieren zu können. Das veranlasste uns, das Papier auch auf Englisch zur Verfügung zu stellen. Was wir gelernt haben: Unsere Behörde hat bereits essentielle Expertise im Bereich KI. Die hiesigen Unternehmen und Behörden können diese Expertise nutzen, die ihnen vor Ort und zugänglich angeboten wird.

Wir danken allen Beteiligten für den konstruktiven Austausch und die wertvolle Kritik. Die Rückmeldungen werden von uns im Haus diskutiert und in der Veröffentlichung einer Version 2.0 des Papiers berücksichtigt.

Digitalgipfel 2023 – Wirtschaft 4.0 BW

Datenschutz und Digitalisierung gehören zusammen: Das Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg hat im Jahr 2023 in Stuttgart wieder den Digitalgipfel BW 2023 veranstaltet, in dessen Mittelpunkt die Digitalisierung der Wirtschaft in Baden-Württemberg stand. Hierbei konnten sich Vertreter_innen aus der Wirtschaft, der Forschung und der Politik über aktuelle Trends der Digitalisierung in der Wirtschaft sowie über neue Innovationen informieren und sich miteinander vernetzen. Ebenso wurden zahlreiche nationale und internationale Expert_innen eingeladen, um gemeinsam über Digitalisierung und Innovationen zu sprechen.

Wir haben in diesem Jahr erstmals an der Veranstaltung teilgenommen, um den circa 3.000 Besucher_innen die Herausforderungen und Potenziale des Datenschutzes in der Digitalisierung aufzuzeigen. Dazu hat unsere Dienststelle einen Informationsstand angeboten, an dem Intressierte mit uns in den direkten Austausch treten konnten. Gleichzeitig haben wir die Möglichkeit wahrgenommen, auf der Hauptbühne einen Impulsvortrag zum Thema „Datenschutz in der Digitalisierung – Balance zwischen Innovation und Privatsphäre“ zu halten, um auf die herausragende Bedeutung des Datenschutzes in der Digitalisierung aufmerksam zu machen.

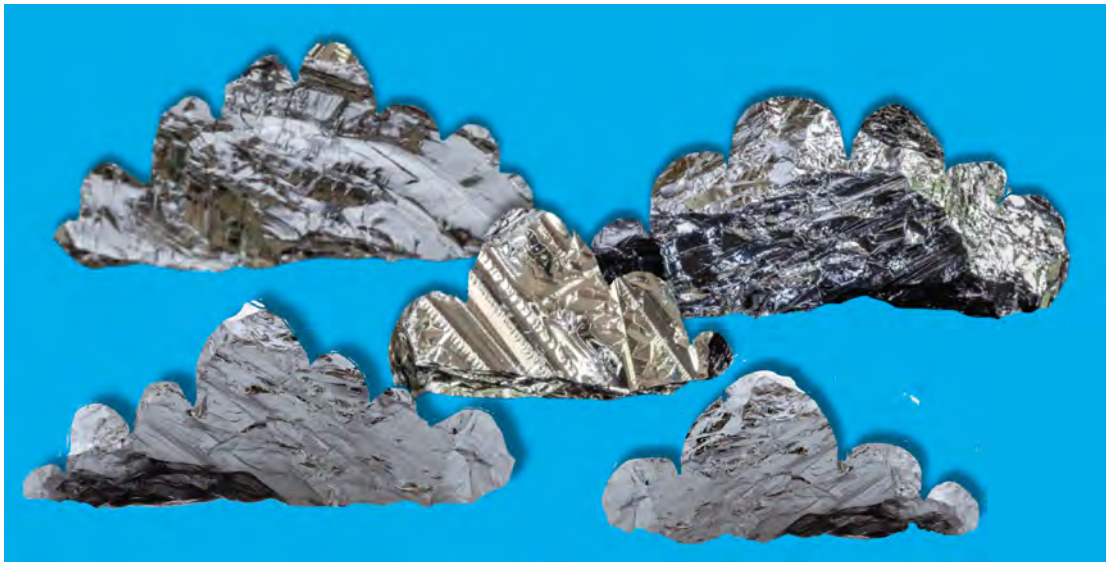
Bei der Entwicklung und Verwendung neuer digitaler Technologien wie etwa im Bereich der KI werden regelmäßig große Mengen an (personenbezogenen) Daten in Form von Trainings- und Anwendungsdaten benötigt. Die Qualität der Digitalisierungsprozesse hängt mitentscheidend von der zugrundeliegenden Datenquantität und Datenqualität ab. Sofern hierbei personenbezogene Daten verarbeitet werden, gelten die Anforderungen der DS-GVO. Datenschutz wird spätestens jetzt für Verantwortliche zum Compliance-Thema.

Es wäre aber zu kurz gedacht, Datenschutz nur als Compliance-Thema zu behandeln. Vielmehr bie-

tet Datenschutz darüber hinausgehend gerade im Bereich der Digitalisierung viele Potenziale. Datenschutz kann als eine Chance für mehr Sicherheit, mehr Innovation und als stärkendes Vertrauensverhältnis zu Kund_innen verstanden werden. Zum einen trägt Datenschutz zur Steigerung der Cybersicherheit bei. Die entsprechende gesetzliche Pflicht, Produkte stets auf dem aktuellen Stand der Technik zu halten, schafft somit neue Anreize, um bestehende Produkte weiterzuentwickeln und neue Innovationen hervorzubringen. Zum anderen wirken die bestehenden datenschutzrechtlichen Vorgaben den Gefahren von Datenmissbräuchen entgegen und steigern so die Produktsicherheit. Gepaart mit datenschutzrechtlichen Transparenzpflichten beispielsweise ergibt sich hieraus die Chance, das Vertrauensverhältnis zur Kundschaft nachhaltig zu stärken und dadurch langfristige Geschäftsbeziehungen aufzubauen.

Datenschutz ist also ein wesentlicher Baustein für eine nachhaltige und innovationsstarke Digitalisierung. Eine wichtige Aufgabe von uns ist es daher, Datenschutz und Digitalisierung zusammenzubringen, um so eine nachhaltige datenschutzkonforme technische Entwicklung zu fördern, auch im Bereich von innovativen Technologien wie etwa bei der Künstlichen Intelligenz.

Hierzu sind wir für alle Interessierten ansprechbar in Sachen Datenschutz, Digitalisierung und KI. Eine besondere Bedeutung in diesem Zusammenhang hat die datenschutzrechtliche Beratung von Start-up-Unternehmen. Denn Gründer_innen stehen regelmäßig nicht nur vor unternehmerischen Herausforderungen, sondern auch vor zahlreichen datenschutzrechtlichen Fragestellungen, mit denen sie sich aktiv auseinandersetzen müssen. Oftmals fehlt es aber an der notwendigen datenschutzrechtlichen Expertise. Es ist daher besonders wichtig, dass gerade in der Gründungsphase eines jungen Unternehmens der Datenschutz bereits von Anfang an mitgedacht wird, weshalb wir genau hier einen Schwerpunkt setzen und Start-ups begleiten wollen. Wir werden hierzu unser Beratungs- und Schulungsangebot für junge Unternehmen weiter ausbauen und unsere Zusammenarbeit mit den Digitalisierungsakteuren aus Baden-Württemberg wie etwa dem Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg intensivieren. Und warum nicht im Innovation Park Artificial Intelligence Heilbronn (Ipai) mit



Catherine Breslin & Tania Duarte / Better Images of AI / AI silicon clouds collage / CC-BY 4.0

Cloudanwendungen sind immer wieder ein Thema für den LfDI.

Bilder: LfDI BW

Wie soll die KI-Verordnung der EU aussehen? Diskussion im Juli 2023 mit Tobias Haar, Rolf Schwartmann, Kai Zenner, Tobias Keber und Axel Voss (v.l.n.r.), moderiert von der LfDI-Referentin Clarissa Henning.

einer kleinen Außenstelle vertreten sein, um noch niederschwelliger Start-upper zu beraten?

Die Zukunft des Datenschutzes – Ist die DS-GVO bereit für KI?

Am 13. Juli 2023 hatte unser Bildungszentrum einen Diskussionsabend in unseren Diensträumen geplant. – zwei Wochen, nachdem der neue Landesbeauftragte seinen Dienst angetreten hatte. Wir befassten uns an diesem Abend mit der hochaktuellen Diskussion über die Ausgestaltung des Europäischen Gesetzes über Künstliche Intelligenz, also die KI-Verordnung (KI-VO).

Als Diskutanten waren der Europaabgeordnete Axel Voss, Tobias Haar (Chefsyndikusanwalt der Aleph Alpha GmbH, Heidelberg), Medien- und Datenschutzrechtler der TH Köln und Vorsitzender der GDD Prof. Dr. Rolf Schwartmann und Kai Zenner (Berater Digitalpolitik des MdEP Axel Voss, zuständig unter anderem für die Ausgestaltung der KI-VO) eingeladen. Geleitet wurde die Diskussion von der persönlichen Referentin des Dienststellenleiters Clarissa Henning. Mit den Podiumsgästen erörterten wir die Rolle und Wirkung der DS-GVO in Bezug auf Anforderungen zukunftsfähiger KI-Technologien.

Die kontroverse Diskussion des Abends zeichnete das Spannungsfeld nach zwischen dem Verständnis der DS-GVO „als Goldstandard“ europäischer Digitalpolitik und einem Beispiel für eine angstgetriebene Regulierung, die Innovationen wie KI bremse. Trotz der auch kritischen Sicht einiger Diskutanten auf die „gelebte“ Regulierung und Auslegung der DS-GVO, waren sich alle Anwesenden doch einig, dass informationelle Selbstbestimmung als demokratiesicherndes Element in einer digitalisierten Gesellschaft notwendig ist, ohne dass die EU im Wettlauf um eine globale KI-Vorreiter-Position auf das Abstellgleis geschoben wird.

Der Abend zeigte die Wichtigkeit, sich gerade auch mit kritischen Stimmen auseinanderzusetzen, um den Datenschutz zu stärken und weiterzuentwickeln. Vielen Dank an unser Bildungszentrum, das nicht nur exzellente Schulungen und Fortbildungen organisiert, sondern auch einen solchen Abend sehr erfolgreich verwirklicht hat. Die Stühle vor Ort waren alle belegt, online hatten wir viele Zuschauende und das Video, welches auf unserem Videoserver nachgeschaut werden kann, verzeichnet bisher über 6.500 Aufrufe.

☛ **Die Zukunft des Datenschutzes – Ist die DS-GVO bereit für KI?**

tube.bawü.social/w/pj4h8hUuHxjfrQd9sFgmm7

Veranstaltungsplakat zur KI-Woche 2023.

KI-Woche beim LfDI

Vom 4. Oktober bis 6. Oktober fand unter dem Titel „Menschendaten. Die Maschine spricht – wer verantwortet KI?“ zum zweiten Mal eine KI-Themenwoche in unserer Dienststelle statt. Wir haben Bürger_innen, Unternehmen und öffentliche Stellen aus Baden-Württemberg eingeladen, um mit uns über Künstliche Intelligenz (KI) in den Austausch zu kommen.

Die hohen Teilnahmezahlen (durchgehend rund 50 Personen vor Ort und bis zu 110 Personen online) zeigten, dass unser Programm auf ein breites Interesse stößt. Das hybride Format hat sich für uns bewährt, der Livestream ist für unsere Veranstaltungen nicht mehr wegzudenken. Um möglichst viele Personen mit unserem Programm zu erreichen, haben wir zahlreiche Vorträge auf unserem Videoserver PeerTube zur Verfügung gestellt, die zusammengenommen mehrere Tausend Aufrufe verzeichnen.

Sowohl unsere Kolleg_innen im Haus als auch die externen Teilnehmenden haben aus der KI-Woche viele Erkenntnisse mitgenommen. Die Wissenschaftler_innen konnten uns die aktuellen technischen und rechtlichen Entwicklungen näherbringen. In der sich rasant verändernden Welt ist dies von unschätzbarem Wert, um unsere eigene Arbeit fundiert leisten zu können.

Sehr verschiedene Disziplinen waren vertreten: Von der IT-Sicherheitsforschung bis zu philosophischen Einordnung nebst Streitgespräch konnten wir uns dem Thema Künstliche Intelligenz aus ganz unterschiedlichen Perspektiven nähern. Doch auch die Anwendung wurde in den Blick genommen. So wurde uns von Unternehmen aus Baden-Württemberg gezeigt, wie sich KI im unternehmerischen Alltag einsetzen lässt. Wir konnten dabei die Potenziale und auch die Herausforderungen beim Einsatz von KI reflektieren. Durch die vielen Gespräche nicht nur mit den Vortragenden, sondern auch mit Teilnehmenden und der Teilnehmenden untereinander wurden vielfältige Blickwinkel auf den Einsatz von KI möglich. Gerade die Interdisziplinarität der Gespräche und Sichtweisen war sehr bereichernd.

Dies ist aus unserer Sicht nicht nur für das Verständnis der KI selbst wichtig, sondern auch für einen effektiven Datenschutz. Nur wenn wir Potenziale und Herausforderungen kennenlernen, die Einsatzgebiete abstecken können und die Perspektiven der Verantwortlichen, aber auch der betroffenen Nutzenden adressieren, können wir zusammen mit den Verantwortlichen praktikable und grundrechtswahrende Lösungen entwickeln. Wir möchten auch in Zukunft mit der breiteren Öffentlichkeit und den vielfältigen Anwender_innen von KI ins Gesprächen kommen und einen offenen Austausch darüber führen, wie KI sinnvoll genutzt werden kann und wo sie reguliert werden sollte oder muss.

Wie bereichernd die KI-Woche war, soll im Folgenden mit einigen kursorischen Betrachtungen erläutert werden.

> ☛ **KI-Woche vom 4.–6. Oktober 2023**
>
> Program der KI-Woche „Menschendaten. Die Maschine spricht – wer verantwortet KI?“ vom 4.–6. Oktober 2023
>
> www.baden-wuerttemberg.datenschutz.de/ki-woche-2023
>
> Vorträge und Diskussionen der KI-Woche vom 4.–6. Oktober 2023:
>
> tube.bawü.social/c/ki_woche_lfdi/videos

Der erste Tag: KI trifft Kunst und Gesellschaft

Am ersten Tag haben wir uns intensiv den gesellschaftlichen Auswirkungen von KI gewidmet – und einen Auftakt gewählt, der den Blick geweitet hat. Wir haben mit einem Blick auf KI durch künstlerische Aneignung begonnen. Dr. Daniel Bisig und Prof. Ephraim Wegner befassen sich bei „Puppeteering AI“ mit der Entwicklung einer virtuellen Puppe, die zur Mitspielerin in Tanz- und Musiktheateraufführungen wird. Sie verfügt über ein Bewegungsrepertoire, das sie sich anhand von Aufnahmen eines realen Tänzers über maschinelles Lernen angeeignet hat. Über Sensoren kann ihre Bewegung auf der Leinwand nun von Spieler_innen (Tänzer_innen während eines Theaterprojektes oder, so wie

bei uns, Interessierten aus dem Publikum) in ihrer Ausrichtung beeinflusst werden. Dies geschieht nicht ganz linear, sodass eine Fremdheit zwischen der eigenen Bewegung und der Bewegung des virtuellen Gegenübers bestehen bleibt. Die Installation war während der gesamten Themenwoche vor Ort begehbar und das Publikum nutzte ausführlich die Gelegenheit, mit der Puppe in Interaktion zu gehen.

Im Anschlusspanel gingen Dr. Carsten Orwat vom KIT und die als „KI-Newcomerin des Jahres 2023" ausgezeichnete Paola Lopez, die an der Universität Wien und am Weizenbaum-Insitut Berlin arbeitet, der Frage nach, wie wir damit umgehen, dass KI immer auch das Potenzial zur Diskriminierung beinhaltet: Liegt ein sogenannter Bias, eine Verzerrung, in gewisser Weise in der Logik maschinellen Ler-

Biasses können über KI reproduziert werden. Hier ein illustratives Beispiel: Ein Mädchen spielt Fußball, ein Junge spielt mit einer Puppe. Durch einen Bias wird dem Mädchen die Puppe und dem Jungen der Fußball zugeschrieben.

Illustrationen von Yasmin Dwiputri für "The Data Hazards Projekt".

nens, da dieses auf Mustererkennung basiert und deshalb stark typisiert, wenn nicht stereotypisiert? Was bedeutet dies für die Anwendungsfelder von KI – wo trauen wir ihren Prognosen und nehmen gewisse und zu minimierende Fehlerquoten als Gesellschaft in Kauf? Was bedeutet eine falsche Prognose für die betroffenen Einzelnen?

Von beiden Vortragenden wurde auf prominente und gerichtlich gekippte Anwendungen verwiesen, in welchen Personenmerkmale mit anderen Merkmalen kombiniert wurden (beispielsweise Wohnadresse mit statistischer Rückfallquote). Wie kann ein Bias bestmöglich minimiert werden und welche „Unschärfen" in der Prognose möchte eine Gesellschaft tolerieren? Hier wurde insbesondere auch deutlich, wie verschieden die Sichtweisen auf das Thema Diskriminierung durch KI sein können und wie mögliche Lösungsansätze für diskriminierungsarme KI aussehen können. Eine Herausforderung, mit der wir sicherlich in Zukunft noch häufiger umgehen werden. Der Tag endete mit regem Austausch zwischen den Vortragenden und dem Publikum.

Der zweite Tag: KI in der IT, Gesundheit, Verwaltung und in Unternehmen

Prof. Dr. Christoph Sorge von der Universität des Saarlandes sprach zu Beginn des zweiten Tages von den Herausforderungen bei KI aus Sicht des technischen Datenschutzes. Sorges Forschungsgebiet ist die Schnittstelle von Informatik und Recht; Schwerpunkte dabei sind technische und rechtliche Aspekte des Datenschutzes. Anhand zahlreicher Beispiele erhielten wir spannende Einblicke in die Herausforderungen des Datenschutzes im Kontext aktueller KI-Anwendungen und bekamen offene Fragen wie auch vielversprechende Lösungsansätze – beispielsweise im Kontext Anonymisierung / Deanonymisierung – skizziert.

Anschließend trugen zur Zukunft der Gesundheitsdatenforschung und der Nutzung von Gesundheitsdaten für maschinelles Lernen die Ärztin Prof. Dr. Melanie Börries vom Universitätsklinikum Freiburg und der Neurowissenschaftler Prof. Dr. Aldo Faisal (Universität Bayreuth und Imperial College London) vor. Beide berichteten über ihre Forschung und über Anwendungsbereiche von KI bei Gesundheitsdaten. Wie kann etwa KI helfen, Krankheiten frühzeitig zu erkennen? Wie stehen KI-Anwendungen, Gesundheitsdatenforschung und IT-Sicherheit zueinander? Was bedarf es aus der Perspektive der IT-Sicherheit und des Datenschutzes, damit der Einsatz von KI in der Gesundheitsdatenforschung für Menschen vertrauenswürdig ist? In der anschließenden Podiumsdiskussion brachte die IT-Sicherheitsexpertin Bianca Kastl in die Anwendungsbeispiele eine neue Perspektive und lenkte den Fokus auf technische und organisatorische Fragen: Im Falle einer Verknüpfung von Gesundheitsdaten und personenbezogenen Verhaltensdaten beispielsweise aus Fitness-Trackern verlange die IT-Sicherheit eine dezentrale Verarbeitung, um Angriffs- und Schadensrisiken verteilen und minimieren zu können.

Der Nachmittag startete mit einem Schwenk in die Verwaltung und Justiz. Björn Beck kam aus dem Justizministerium und berichtete von zahlreichen Initiativen in Baden-Württemberg, welche zurzeit im Bereich der Justiz entwickelt werden und welche zum Teil auch schon in der Praxis erprobt werden. Anschließend berichtete Martin Reisinger vom InnoLab_bw, dem Innovationslabor des Staatsministeriums, vom Pilotprojekt F13: Das Programm ist eine KI-Anwendung für den Einsatz in der Verwaltung, um dort Arbeitsprozesse zu erleichtern.

Am Nachmittag gab es im besten Sinne des Wortes einen Streit: Es ging um die Frage, ob Maschinen wie Menschen tatsächlich „sprechen". Es kamen drei Wissenschaftler_innen zum titelgebenden und wieder eher allgemeineren Thema zusammen: Was können Sprachmodelle und was können sie nicht? Prof. Dr. Hannah Bast ist Mathematikerin und Informatikerin, sie baut schon länger (lernende und nichtlernende) technische Informationssysteme. Prof. Dr. Thomas Fuchs ist Philosoph, Psychiater und Erich-Fromm-Preisträger 2023 und sieht die Herausforderung v. a. darin, Maschinen und Menschen nicht in eins zu setzen. Für ihn ist evident, dass Maschinen niemals wie Menschen Zugang zu Sinn und Bedeutung haben können. Auf den Unterschied, wie Maschinen und Menschen

Informationen erfassen oder Objekte „wahrnehmen", machte wiederum Prof. Felix Wichmann, Dhil, ausgewiesener Spezialist auf dem Gebiet der Neuronalen Informationsverarbeitung, aufmerksam: Statt Gegenständen „registrierten" Maschinen eher Oberflächenstrukturen. Nach den jeweiligen Kurzimpulsen diskutierten Bast, Wichmann und Fuchs unter dem Titel „Die Maschine spricht (nicht)" intensiv ihre Ansichten zum Thema, es wurden Gemeinsamkeiten und unterschiedliche Auffassungen deutlich: Es war ein Erkenntnis bringender intensiver interdisziplinärer Austausch.

Zum Abschluss des Tages traf KI dann auf Unternehmen, wir lernten Dr. Jan Oevermann, den Geschäftsführer der plusmeta GmbH, kennen. Das baden-württembergische Unternehmen hat eine KI-Anwendung entwickelt, die verstecktes Wissen aus Datenbergen holt. Die KI-Lösung ermöglicht es Anwender_innen somit, die notwendigen Prozesse für eine Sichtung und Aufbereitung ihrer Daten effektiver zu gestalten. Jan Overmann erklärte uns, wie plusmeta funktioniert, für welche Anwendungsfelder die KI-Lösung eingesetzt werden kann, wo aber auch noch Herausforderungen für die Praxis und für den Datenschutz liegen.

Der dritte Tag: Workshops & Europa im Fokus

Am letzten Tag der Themenwoche konnten alle Interessierten vor Ort an Workshops teilnehmen. Sie sollten eine Möglichkeit bieten, niederschwellig mit unseren Referent_innen in Kontakt zu kommen und so die Arbeit des Landesbeauftragten besser kennenzulernen. Die Workshops waren so konzipiert, dass ohne weiteres Vorwissen teilgenommen werden konnte. Sie wurden ein voller Erfolg, nicht nur waren die Workshops ausgebucht, sondern es kam auch zu intensivem Austausch.

Workshop 1 „Die Zukunft des (kassenlosen) Einkaufens – Grab and Go?" – Johannes Rembold, LL.M., teilte hier sein Wissen zum kassenlosen Einkaufen und den datenschutzrechtlichen Implikationen mit Interessierten. Workshop 2 lautete „Datenschutzrechtliche Aspekte bei KI-Systemen". KI-Systeme verarbeiten oftmals personenbezogene Daten. Wie sieht es mit den Rechtsgrundlagen für diese Verarbeitungen aus? Kollege Daniel Maslewski besprach u. a. Betroffenenrechte. Workshop 3 befasste sich mit „Urteil KI – Betroffenenrechte / Intransparenz / Bias". Hier sprach Dr. Peter Nägele über den vielfältigen Einsatz von KI in staatlichen, behördlichen oder Bildungskontexten bei Bestimmung von Schulnoten, Aufdeckungsbestrebungen von Sozialhilfebetrug, Terrorismusbekämpfung oder Wiedereingliederung in den Arbeitsmarkt. In Workshop 4 zeigte Dr. Kristof Meding unter dem Titel „Vergleich und Funktionsweise von Sprachmodellen" verschiedene Sprachmodelle im Einsatz und erkundete im Austausch mit den Teilnehmenden Unterschiede im Gebrauch und im Reifegrad der Technik. Die Informationsfreiheit spielte im Workshop 5 „Kein Bock auf LIFG? Kolleg_in KI hilft!" die zentrale Rolle. Informationsbereitstellung schafft einen Mehrwert für Bürger_innen und unterstützt demokratische Partizipation. KI kann bei der Suche nach Informationen unterstützen. Unsere Kolleginnen Sabine Grullini, Michela Iuliano und Team lieferten Wissenswertes.

Zum Abschluss am Mittag rückte Europa in den Fokus. KI entwickelt sich rasend schnell. Gesetze brauchen lange. Prof. Dr. Hannah Ruschemeier sprach über „Experimentelle Regulierung als effektive KI-Governance" mit Beispielen der sogenannten Sandbox-Systeme. Zu ihren Forschungsschwerpunkten zählen Gefährdungen von Grundrechten durch neue Technologien, rechtstheoretische Grundlagen der Digitalisierung sowie Datenschutzrecht. Sie diskutierte im Anschluss an ihren Vortrag mit dem Dienststellenleiter, sowie seinem Vorgänger Dr. Stefan Brink, der heute das Wissenschaftliche Institut zur Digitalisierung der Arbeitswelt wida in Berlin leitet, Dr. Boris Paal, Professor für Bürgerliches Recht und Informationsrecht, Daten- und Medienrecht. In der Diskussion wurde deutlich, welche Herausforderungen es bei der effektiven KI-Regulierung noch gibt und welche Auswirkungen der Einsatz von Künstlicher Intelligenz auf Privatheit und Freiheit hat.

Im Herbst 2024 findet die dritte KI-Woche statt. Wir freuen uns darauf.

Aktuelle Entwicklungen im Beschäftigtendatenschutz

Im Berichtsjahr hatten wir einige datenschutzrechtliche Fragen beim Beschäftigtendatenschutz auf dem Tisch. Erwartbar stellt der Einsatz von KI weitere, zum Teil neue Fragen, die beantwortet werden müssen. Wir alle warten darauf, dass die im Bund angekündigte Novellierung des Beschäftigtendatenschutzgesetzes auch tatsächlich kommt. Das Bundesinnenministerium (BMI) und das Bundesarbeitsministerium (BMAS) hatten im April 2023 in einem gemeinsamen Papier Eckpunkte eines neuen Beschäftigtendatenschutzgesetzes vorgestellt. Wir werden uns jedenfalls im Jahr 2024 mit dem Einsatz von KI im Beschäftigtenkontext auseinandersetzen und ferner anlassbezogene und anlasslose Kontrollen beim Einsatz von KI im Beschäftigtenverhältnis durchführen.

FAQ zum Urteil des Europäischen Gerichtshofs vom 30. März 2023

Das Urteil des Europäischen Gerichtshofs vom 30. März 2023 (Az. C-34/21) hat den Bereich des Beschäftigtendatenschutzes im Jahre 2023 erheblich beschäftigt. In ihm hat sich der EuGH erstmals zur Umsetzung des Art. 88 DS-GVO im deutschen Beschäftigtendatenschutz geäußert. Die DSK hat eine Entschließung zu diesem Urteil verabschiedet und wir haben im September 2023 FAQ zu den Auswirkungen des Urteils veröffentlicht.

Nationale Gesetzgeber dürfen im Anwendungsbereich der DS-GVO grundsätzlich nicht tätig werden, da diese als Verordnung den Bereich abschließend regelt und nicht von den Mitgliedsstaaten umgesetzt werden muss. Der nationale Gesetzgeber darf sich weder in Widerspruch zu den vorrangigen Regelungen der DS-GVO setzen noch diese in sein nationales Recht übernehmen. Allerdings enthält die DS-GVO Normen, die dem nationalen Gesetzgeber den Erlass von Regelungen gestatten, sog. Öffnungsklauseln. Die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext kann nach Art. 88 Abs. 1 DS-GVO durch die Mitgliedstaaten geregelt werden. Auf diese Vorschrift wurden u. a. die Generalklauseln im Beschäftigtendatenschutz gestützt, die die Verarbeitung von Beschäftigtendaten erlauben, wenn dies für die Eingehung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist. In Baden-Württemberg sind dies konkret § 26 Abs. 1 Satz 1 BDSG für den nicht-öffentlichen Bereich und § 15 Abs. 1 Satz 1 LDSG für den öffentlichen Bereich sowie § 83 Abs. 1 LBG für Personalaktendaten im öffentlichen Dienst.

Das Verwaltungsgericht Wiesbaden hatte Zweifel daran, ob die den zuvor genannten Normen vergleichbare Generalklausel zum Beschäftigtendatenschutz im hessischen Datenschutzgesetz, § 23 Abs. 1 Satz 1 HDSIG, den Anforderungen des Art. 88 Abs. 1 und 2 DS-GVO genügt. Daher befragte es den EuGH zur Auslegung dieser Norm. Der EuGH stellte klar, dass Art. 88 Abs. 1 DS-GVO, der „spezifischere Vorschriften" voraussetzt, verlangt, dass die auf ihn gestützten Normen nicht nur Anforderungen wiederholen, die die DS-GVO bereits für sämtliche Datenverarbeitungen aufstellt. Wenn in der DS-GVO Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind, können die Mitgliedstaaten zwar nach Erwägungsgrund 8 Teile dieser Verordnung in ihr nationales Recht aufnehmen, soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen. Dies bedeutet aber nicht, dass die Vorschriften den Rahmen, welchen die Öffnungsklausel vorgibt, nicht mehr einhalten müssen. Außerdem müssen die nach Art. 88 Abs. 1 DS-GVO erlassenen Vorschriften gem. Art. 88 Abs. 2 DS-GVO geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen. Bestimmungen, die die Verarbeitung personenbezogener Beschäftigtendaten davon abhängig machen, dass

Bild: MarutStudio-stock.adobe.com

Beschäftigtendatenschutz wird in KI-Zeiten immer wichtiger.

diese zu bestimmten Zwecken im Zusammenhang mit der Durchführung eines Beschäftigungs- bzw. Dienstverhältnisses erforderlich sein muss, scheinen nach dem EuGH die bereits in Art. 6 Abs. 1 UnterAbs. 1 Buchst. b DS-GVO aufgestellte Bedingung für die allgemeine Rechtmäßigkeit der Verarbeitung zu wiederholen, ohne eine spezifischere Vorschrift i.S.v. Art. 88 Abs. 1 DS-GVO hinzuzufügen.

Diese Vorschriften können damit nicht auf Art. 88 Abs. 1 DS-GVO gestützt werden, sie sind nur dann weiterhin anwendbar, wenn sie auf eine andere Öffnungsklausel gestützt werden können. Der EuGH hat hier die Öffnungsklausel des Art. 6 Abs. 3 DS-GVO betrachtet. Diese setzt jedoch voraus, dass die in der nationalen Vorschrift geregelte Datenverarbeitung entweder zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe bzw. in Ausübung öffentlicher Gewalt erfolgt (vgl. Art. 6 Abs. 1 UnterAbs. 1 Buchst. e DS-GVO) oder der Verantwortliche zur Datenverarbeitung verpflichtet wird (vgl. Art. 6 Abs. 1 Unterabs. 1 Buchst. c DS-GVO). Die Ermächtigung zur Verarbeitung von Beschäftigtendaten für Zwecke des Beschäftigungsverhältnisses durch private, nicht mit im öffentlichen Interesse liegenden Aufgaben betraute Arbeitgeber erfüllt diese Voraussetzungen nicht. Damit ist § 26 Abs. 1 Satz 1 BDSG für diese nicht mehr anwendbar und die bislang auf diese Norm gestützten Datenverarbeitungen benötigten eine andere Grundlage. Diese liegt hierbei in Art. 6 Abs. 1 Unterabs. 1 Buchst. b DS-GVO, wenn die Datenverarbeitungen zur Erfüllung des Arbeitsvertrags mit der betroffenen Person oder, bei Bewerbungen, für vorvertragliche Maßnahmen auf Anfrage der betroffenen Person erforderlich sind. Andere Rechtsgrundlagen zur Verarbeitung von Beschäftigtendaten wie § 26 Abs. 1 Satz 2 BDSG oder Art. 6 Abs. 1 Unterabs. 1 Buchst. c DS-GVO i. V. mit der zur Datenverarbeitung verpflichtenden Norm bleiben weiterhin anwendbar.

Im öffentlichen Bereich kann die Verarbeitung von Beschäftigtendaten weiterhin auf § 15 Abs. 1 Satz 1 LDSG gestützt werden und auch § 83 Abs. 1 LBG ist für die Verarbeitung von Personaldaten wei-

ter anwendbar. Wie der EuGH in dem Urteil angedacht hat, liegen die Datenverarbeitungen, die dafür erforderlich sind, dass die im öffentlichen Bereich tätigen Personen ihre Arbeitsleistung erbringen können, im öffentlichen Interesse i.S.v. Art. 6 Abs. 1 Unterabs. 1 Buchst. e DS-GVO. Daher ist Art. 6 Abs. 3 DS-GVO eine taugliche Grundlage für Normen zur Verarbeitung von Beschäftigtendaten im öffentlichen Bereich. Diese müssen dann lediglich nach Art. 6 Abs. 3 Satz 4 DS-GVO in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Ob auch die Voraussetzungen des Art. 6 Abs. 3 Satz 3 DS-GVO zu erfüllen sind, richtet sich nach dem Bestimmtheitsgebot.

☛ Mehr Infos

Rechtsgrundlagen bei Beschäftigtendaten – FAQ zum EuGH, Urteil vom 30. März 2023, Az. C-34/21:
www.baden-wuerttemberg.datenschutz.de/faq-rechtsgrundlagen-bei-beschaeftigtendaten

Entschließung der DSK „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!":
datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

FAQ zum Hinweisgeberschutzgesetz

Zum 1. Juli 2023 ist das Hinweisgeberschutzgesetz (HinSchG) in Kraft getreten. Bereits im Vorfeld gingen viele Anfragen zu einer datenschutzrechtskonformen Umsetzung des Gesetzes bei uns ein. Auch im Gesetzgebungsverfahren zum baden-württembergischen Gesetz über die Einrichtung und den Betrieb einer internen Meldestelle durch Gemeinden und Gemeindeverbände und solche Beschäftigungsgeber, die im Eigentum oder unter der Kontrolle von Gemeinden oder Gemeindeverbänden stehen, wurden wir einbezogen. Um zur Klärung der vielfältigen und viel diskutierten datenschutzrechtlichen Rechtsfragen im Zusammenhang mit dem HinSchG und der nach § 12 HinSchG einzurichtenden internen Meldestelle beizutragen, haben wir im Oktober 2023 FAQ zu diesem Thema veröffentlicht.

Hierin beschäftigen wir uns u. a. mit den Anforderungen an eine interne Meldestelle und die in Frage kommenden Ausgestaltungsmöglichkeiten der datenschutzrechtlichen Verantwortlichkeit bei ihrer Einrichtung. Die mit den Aufgaben einer internen Meldestelle beauftragten Personen müssen nach § 15 Abs. 1 HinSchG unabhängig sein. Sie dürfen neben ihrer Tätigkeit für die interne Meldestelle andere Aufgaben und Pflichten wahrnehmen. Es ist dabei sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu Interessenkonflikten führen. Gem. § 15 Abs. 2 HinSchG müssen sie über die zur Erledigung der Aufgabe notwendige Fachkunde verfügen. Im Zusammenhang mit dem Datenschutzrecht wird insbesondere die Frage ob behördliche oder betriebliche Datenschutzbeauftragte mit dem Betrieb der internen Meldestelle beauftragt werden können. diskutiert. Diese Möglichkeit wird von der Gesetzesbegründung zum HinSchG vorgesehen und ist sowohl nach Art. 38 Abs. 6 DS-GVO als auch nach § 15 Abs. 1 HinSchG zulässig, wenn Interessenkonflikte ausgeschlossen werden. Interessenkonflikte entstehen, wenn die interne Meldestelle Meldungen von Verstößen gegen die DS-GVO nachgeht, da diese in den Bereich der Datenschutzbeauftragten fallen, und wenn sie Datenverarbeitungen kontrollieren müssen, über deren Zweck und Mittel sie als interne Meldestelle selbst unabhängig und weisungsfrei entschieden haben. In beiden Fällen müsste die Person mit der Doppelfunktion als Datenschutzbeauftragte und interne Meldestelle ihr eigenes Verhalten bewerten, was nicht neutral möglich ist. Dementsprechend dürfte ohne ergänzende Maßnahmen eine solche Doppelfunktion einen grundsätzlichen Interessenkonflikt darstellen. Nach der Rechtsprechung des EuGH ist für die Frage eines konkreten Interessenkonfliktes die Organisationsstruktur des Verantwortlichen, einschließlich interner Vorschriften, maßgeblich (vgl. EuGH, Urteil vom 9. Februar 2023, Az C-453/21, Rz. 46). Hierbei ist eine Einzelfallbetrachtung geboten: Zu berücksichtigende Mindestvoraussetzungen für die Vermeidung eines Interessenkonfliktes wären geeignete Vertretungsregelungen auf beiden Seiten, klare Zuständigkeiten und Rollentrennungen (organisatorisch und sachlich, z. B. bei Aktenführung und Archivierung) sowie eine lückenlose Prozessdokumentation.

Die datenschutzrechtliche Verantwortlichkeit für die von der internen Meldestelle vorgenommenen Datenverarbeitungen hängt wesentlich von der Ausgestaltung des Sachverhalts ab. Wird die Meldestelle durch Mitarbeitende des Beschäftigungsgebers betrieben, ist dieser Verantwortlicher und die Meldestelle lediglich Teil der verantwortlichen Stelle. Wird jedoch gem. § 14 Abs. 1 Satz 1 Var. 2 HinSchG ein Dritter, z. B. ein verbundenes Unternehmen oder eine Anwaltskanzlei, mit dem Betrieb der internen Meldestelle beauftragt, wird dieser hierdurch nicht Teil des Beschäftigungsgebers. Vielmehr ist ein sämtliche Aufgaben der internen Meldestelle übernehmender Dritte ein eigener Verantwortlicher nach Art. 4 Nr. 7 DS-GVO, zwischen ihm und der internen Meldestelle besteht eine gemeinsame Verantwortlichkeit für die vorgenommenen Datenverarbeitungen nach Art. 26 DS-GVO, eine entsprechende Vereinbarung ist abzuschließen. Soll der Dritte der eigentlichen internen Meldestelle lediglich zuarbeiten, z. B. indem er die technischen Voraussetzungen für den Meldekanal bereitstellt oder Meldungen für die interne Meldestelle entgegennimmt, liegt ein Fall der Auftragsverarbeitung nach Art. 4 Nr. 8 DS-GVO und Art. 28 und 29 DS-GVO vor.

Die von der internen Meldestelle vorgenommenen Datenverarbeitungen können auf Art. 6 Abs. 1 Satz 1 Buchst. c DS-GVO i. V. mit §§ 10 und 12 bzw. 16ff. HinSchG gestützt werden. § 12 HinSchG normiert die Pflicht zum Betrieb der internen Meldestelle und § 10 HinSchG regelt die Datenverarbeitung durch diese zur Erfüllung ihrer Aufgaben. § 10 Satz 2 HinSchG enthält auch eine Rechtsgrundlage zur Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 2 Buchst. g DS-GVO. Die Weitergabe der personenbezogenen Daten der hinweisgebenden Person und der in der Meldung genannten Personen richtet sich nach § 18 Nr. 4 und § 9 Abs. 2 bis 4 HinSchG.

Der Schutz der Vertraulichkeit der hinweisgebenden Personen und der in der Meldung genannten Personen nach §§ 8 und 9 HinSchG ist zu beachten und darf auch nicht durch die Pflicht zur Information der betroffenen Personen nach Art. 14 DS-GVO und das Auskunftsrecht der betroffenen Personen nach Art. 15 DS-GVO umgangen werden. Diese sind insoweit durch § 29 Abs. 1 BDSG und ggf. Art. 15 Abs. 4 DS-GVO begrenzt.

Schließlich sind bei der Einrichtung der Meldekanäle und internen Meldestellen die allgemeinen Anforderungen der DS-GVO, wie die Grundsätze des Art. 5 DS-GVO, das Erfordernis technischer und organisatorischer Maßnahmen zum Schutz der Vertraulichkeit der verarbeiteten Daten nach Art. 32 DS-GVO, das Erfordernis einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und die Pflicht zur Einbindung der behördlichen oder betrieblichen Datenschutzbeauftragten nach Art. 38 Abs. 1 DS-GVO zu beachten.

Eine Orientierungshilfe der DSK zum Thema Hinweisgeber-Meldestellen und Beschäftigtendatenschutz befand sich bei Redaktionsschluss noch in Überarbeitung.

☛ **Mehr Infos:**

FAQ Hinweisgeberschutzgesetz:

www.baden-wuerttemberg.datenschutz.de/faq-hinweisgeberschutzgesetz

EuGH, Urteil vom 9. Februar 2023, Az. C-453/21, Rz. 46:

curia.europa.eu/juris/document/document.jsf?text=&docid=270323&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

FAQ zum Thema Datenschutz in Schwerbehindertenvertretungen

Der LfDI unterstützt die wichtige Arbeit der Schwerbehindertenvertretungen und bietet Antworten auf häufig gestellte Datenschutzfragen bei der Gremienarbeit durch eine FAQ.

Ende 2022 wurden in allen Betrieben und Dienststellen des Landes die Schwerbehindertenvertretungen (SBV) gewählt. Die Schwerbehindertenvertretung hat die Aufgabe, kollektive und individuelle Interessen schwerbehinderter und ihnen gleichgestellter Personen in Beschäftigungsverhältnissen in Betrieb

oder Dienststelle zu vertreten, die Eingliederung dieser Beschäftigten zu fördern und ihnen beratend und helfend zur Seite zu stehen. Die Arbeit der SBV ist damit ein unverzichtbarer Beitrag zur Inklusion der betroffenen Personengruppen in die Arbeitswelt.

Die Tätigkeiten der SBV sind u. a. durch die fortschreitende Digitalisierung betrieblicher und behördlicher Arbeitsweisen stetem Wandel unterworfen. Der Datenschutz ist hierbei elementarer Bestandteil der Arbeit in der SBV: Mitarbeitende müssen zum einen darauf vertrauen können, dass ihre personenbezogenen Daten bei der SBV gut aufgehoben sind; zum anderen ist die SBV auch gesetzlich verpflichtet, sich bei ihrer Arbeit datenschutzkonform zu verhalten.

Das Informationsbedürfnis der Schwerbehindertenvertretungen hat sich im vergangenen Jahr – nicht zuletzt auch aufgrund der oben bereits angesprochenen Neuwahl sämtlicher Schwerbehindertenvertretungen des Landes und durch Aufnahme der Arbeit der neu gewählten Interessenvertretungen – als hoch erwiesen. Schon in der Vergangenheit haben wir bestehenden Unsicherheiten mit Vorträgen und in der Beratungspraxis Rechnung getragen.

Gerade in der täglichen Umsetzung ergeben sich für die SBV immer wieder eine Vielzahl datenschutzrechtlicher Fragen; insbesondere die Frage, wie die Arbeit datenschutzkonform ausgestaltet werden kann, treibt die Praxis um. Hierbei greifen wir den Schwerbehindertenvertretungen unter die Arme: Für zahlreiche Fälle gibt der von uns neu veröffentlichte Frage-Antwort-Katalog (FAQ) den Schwerbehindertenvertretungen eine erste Hilfestellung, aber auch Orientierung für schwerbehinderte oder diesen gleichgestellte Beschäftigte. Hierdurch können alle Interessierten einen guten Überblick über wesentliche Fragen rund um die Verarbeitung personenbezogener Daten in der täglichen Arbeit der SBV bekommen und Fallstricke erfolgreich gemeistert werden. Unsere FAQ will als ein erster Aufschlag für ein dynamisches, wachsendes Dokument verstanden werden, das in der Zukunft durch weitere Fragen aus unserer Beratungspraxis ergänzt werden kann. Auf diese Weise kann so über die Zeit eine umfangreiche Praxishilfe für die Schwerbehindertenvertretungen entstehen.

☛ **FAQ zum Datenschutz in der Schwerbehindertenvertretung**

www.baden-wuerttemberg.datenschutz.de/faq-datenschutz-in-der-schwerbehindertenvertretung

Die gesellschaftliche Teilhabe aller und damit auch die Arbeit der Schwerbehindertenvertretungen haben einen sehr hohen Stellenwert in unserer Berufswelt. Deshalb ist es uns ein wichtiges Anliegen, die Arbeit der Schwerbehindertenvertretungen mit unserer FAQ zu unterstützen.

Zwei Hochschulen, ein Justitiariat und keine Rechtsgrundlage für die Übermittlung von Personalaktendaten

Zwei baden-württembergische Hochschulen hatten – auch aus haushälterischen Gründen – ein gemeinsames Justitiariat mittels einer Kooperationsvereinbarung eingerichtet. Dies hatte zur Folge, dass in mindestens einem Fall Personalaktendaten der einen Hochschule der anderen Hochschule übermittelt wurden. Dies wurde von uns als rechtswidrig bemängelt, da es hierfür keine Rechtsgrundlage im Landesrecht gibt.

Zwar erlaubt § 12 Abs. 1 Satz 1 Landeshochschulgesetz (LHG) die Verarbeitung personenbezogener Daten, „wenn und soweit die Verarbeitung zur Erfüllung der Aufgaben der Hochschule erforderlich ist." Zudem haben die Hochschulen zur besseren Erfüllung ihrer öffentlichen Aufgaben nach § 6 Abs. 1 Satz 1 LHG zusammenzuwirken. Auch wenn hierdurch im Bereich der gesetzlichen Aufgabenerfüllung unter Umständen auch die Übermittlung personenbezogener Daten zwischen den an einer solchen Kooperation beteiligten Hochschulen legitimiert werden kann, gilt dies zumindest nicht für die Übermittlung von Personalaktendaten. So sieht nämlich § 12 Abs. 10 LHG einen Vorrang der landesrechtlichen Regelungen für Beschäftigten-

daten vor, diese dürfen also nicht auf Grundlage der Generalklausel des § 12 Abs. 1 LHG und damit auch nicht auf Grundlage einer Kooperationsverarbeitung verarbeitet oder übermittelt werden.

Unter welchen Voraussetzungen Personalaktendaten verarbeitet bzw. übermittelt werden dürfen, regeln die §§ 83ff. LBG. Hierbei wiederum genießt § 85 LBG als speziellere Regelung für Datenübermittlungen zwischen öffentlichen Stellen Vorrang vor der personalaktenrechtlichen Generalklausel des § 83 LBG. Vorliegend war aber keine der enumerativen Übermittlungstatbestände erfüllt. Der Vorrang sowohl der spezialgesetzlichen Regelungen für Personalaktendaten im Allgemeinen als auch des § 85 LBG für Übermittlungen im Besonderen gründet in der Sensibilität der betroffenen Daten. So enthalten Personalakten alle Informationen im Zusammenhang mit dem Dienstverhältnis, unter Umständen Führungszeugnis, Bundeszentralregisterauszug, dienstliche Beurteilungen, Disziplinarvorgänge, Unterlagen über die Besoldung und Versorgung, Krankmeldungen (und damit Gesundheitsdaten) u. v. m. Auf Grund dieser besonderen Sensibilität sind Personalakten nach § 50 BeamtStG auch vertraulich zu behandeln.

Als Konsequenz scheiden Kooperationsvereinbarungen nach § 6 LHG als Rechtsgrundlage für die Übermittlung von Personalaktendaten aus, weil eine gesetzliche Ermächtigungsgrundlage für diese Art der Datenverarbeitung in Baden-Württemberg – im Gegensatz zu anderen Bundesländern – fehlt. Hiermit ist keine Aussage hinsichtlich der grundsätzlichen Kooperation zwischen zwei Hochschulen im Bereich der Justitiariate oder der damit einhergehenden Verarbeitung von personenbezogenen Daten verbunden, soweit dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist. In keinem Fall dürfen aber Personalaktendaten übermittelt werden; dies ist durch entsprechende technischen und organisatorischen Maßnahmen sicherzustellen, beispielsweise durch hinreichende Anonymisierung oder Formulierung lediglich allgemeiner Rechtsfragen ohne Personenbezug.

Wir haben die Hochschule aufgefordert, zukünftig Übermittlungen von Personalaktendaten alleine auf Grundlage einer Kooperationsvereinbarung zu unterlassen. Da wir davon ausgehen dürfen, dass die Hochschule dies beachten wird, haben wir von einer formellen Anordnung nach Artikel 58 Abs. 2 DS-GVO abgesehen.

Das Vorgesetztenfeedback

Das Innenministerium setzt – wie auch andere Teile der Landesverwaltung – seit 2018 ein sogenanntes „Vorgesetztenfeedback" als Führungsinstrument ein. Dieses sieht folgendes vor: Die Mitarbeitenden sollen mit einem Online-Fragebogen über die Führungssituation und die Führungsqualitäten ihrer unmittelbaren Vorgesetzten (Führungskraft) befragt werden. Die Teilnahme ist den Mitarbeitenden freigestellt; die Antworten der Mitarbeitenden sollen anonymisiert werden. Zudem kann die Führungskraft entscheiden, ob sie ein solches Feedback durchführen möchte.

Durch dieses Führungsinstrument soll ein Dialog über das Führungsverhalten zwischen der Führungskraft und den Mitarbeitenden ermöglicht werden. Die Führungskraft hat zwingend das Befragungsergebnis mit den Mitarbeitenden zu besprechen. Sie kann zudem eigene Vorgesetzte über die Durchführung des Feedbacks informieren. Mitarbeitende müssen den Inhalt dieses Feedbacks vertraulich behandeln. Um die Anonymität auch während der Auswertung und Präsentation der Ergebnisse zu gewährleisten, ist eine Auswertung nur möglich, wenn mindestens fünf Befragungsteilnehmende ihre Antworten für die Auswertung durch aktives Abschließen der Befragung bereitgestellt haben und sie dann ihre Antworten nicht mehr widerrufen können.

Im Rahmen der Überarbeitung dieses Konzeptes wurden wir nunmehr seitens des Innenministeriums eingebunden und haben dabei verschiedene datenschutzrechtliche Verbesserungsmöglichkeiten aufgezeigt.

So ist die zwingende Verpflichtung, die Ergebnisse der Befragung gegenüber allen Beteiligten vorzustellen, nicht mit den Grundsätzen der Freiwilligkeit

(§ 26 Abs. 2 BDSG) und jederzeitigen Widerruflichkeit (Artikel 7 Abs. 3 DS-GVO) in Einklang zu bringen.

Auch die optionale Information der eigenen Vorgesetzten durch die Führungskraft ist datenschutzrechtlich nicht unproblematisch. Es muss grundsätzlich verhindert werden, dass die Führungskraft Nachteile bei Nichtteilnahme befürchtet, andernfalls könnte sich hieraus ein faktischer Zwang ergeben, so dass eine Freiwilligkeit nicht mehr angenommen werden kann. In diesem Zusammenhang ist die Information der eigenen Vorgesetzten relevant, da erst aus der Information der Vorgesetzten – bzw. den Rückschlüssen, die sich hieraus für die (Nicht-) Teilnahme ergeben – Vor- und Nachteile entstehen können. Dem kann dadurch begegnet werden, dass festgehalten wird, dass die Information der jeweiligen eigenen Vorgesetzten über die Teilnahme am Vorgesetztenfeedback nicht dokumentiert werden soll und den Teilnehmenden hieraus keine dienstlichen Vorteile (und aus einer Nichtteilnahme keine dienstlichen Nachteile) erwachsen dürfen.

Soweit das Konzept von der Anonymität der Befragten ausgeht und hierzu vorsieht, dass nur dann ein Zugang zur Auswertung für die Führungskraft erfolgt, wenn mindestens fünf Mitarbeitende die Befragung abgeschlossen haben, haben wir auf folgendes hingewiesen: Da es sich vorliegend um keine der teilnehmenden Führungsperson unbekannte Gruppe handelt, zudem Freitextfelder individuelle Eingaben ermöglichen, welche eine leichtere Identifizierbarkeit (z. B. durch Rückschlüsse auf Grund gewählter Formulierungen) mit sich bringen, haben wir dem Innenministerium empfohlen, die Gruppengröße zu erhöhen. Außerdem sollte in der Freitexteingabe ausgeschlossen sein, dass sich die Befragten über Dritte äußern können. Eine solche Äußerung würde nämlich eine Verarbeitung personenbezogener Daten dieser dritten Person darstellen, welche der Rechtsgrundlage bedarf. Zudem ist die Ergebnisbesprechung in der Gruppe mit Blick auf die zu gewährleistende Anonymität kritisch zu hinterfragen.

Neben den oben dargestellten rechtlichen Hinweisen haben wir noch verschiedene technisch-organisatorische Verbesserungsvorschläge unterbreitet und alternative Gestaltungsmöglichkeiten aufgezeigt, um das Vorgesetztenfeedback in allen Belangen auf ein gutes datenschutzrechtliches Fundament zu stellen. Unser Rat wurde aufgegriffen. Wir führen unseren Austausch mit dem Innenministerium fort und unterstützen die datenschutzrechtliche Umsetzung.

Aufsichtsverfahren gegen Innenministerium wegen Übermittlung von Personalaktendaten an einen Pressevertreter

Im Mai 2022 erhielten wir eine parlamentarische Anfrage zur datenschutzrechtlichen Bewertung eines Vorgangs im Innenministerium. Ausgangspunkt waren ursprünglich Vorwürfe gegen den Inspekteur der Polizei, welche in ein Disziplinarverfahren mündeten. Im Rahmen dieses laufenden Disziplinarverfahrens hatte dessen Anwalt dem Innenministerium unter anderem den Wunsch zu einem persönlichen Gespräch unterbreitet. Dieses Schreiben war in der Folge durch das Innenministerium an einen einzelnen Journalisten weitergegeben worden. Nach einer öffentlichen Stellungnahme des Innenministers diente diese Weitergabe der Transparenz. Nach pflichtgemäßer Beantwortung der Anfrage (siehe dazu Tätigkeitsbericht 2022, S. 83) leiteten wir ein aufsichtsbehördliches Verfahren nach Artikel 58 DS-GVO ein, welches mit Rücksicht auf staatsanwaltschaftliche Ermittlungen zum gleichen Sachverhalt bis zum förmlichen Abschluss dieser Ermittlungen zurückgestellt wurde. Nach Abschluss des Ermittlungsverfahrens nahmen wir das Verfahren wieder auf und forderten das Innenministerium Baden-Württemberg im Rahmen einer Anhörung zur Stellungname auf. Nach der abschließenden datenschutzrechtlichen Bewertung beendeten wir das Verfahren gegen das Innenministerium Baden-Württemberg mit der Feststellung eines Datenschutzschutzverstoßes nach Artikel 5 Abs. 1 Buchst. a, Artikel 6 Abs. 1 DS-GVO.

Zur Begründung wurde ausgeführt, dass die Übermittlung des Anwaltsschreibens an einen Journalisten datenschutzrechtlich unzulässig war und den Personaldatenschutz verletzt hat. Die Übermittlung konnte nicht auf das Presserecht oder das

Landesinformationsfreiheitsgesetz (LIFG) gestützt werden. Gegenüber diesen Regelungen hatte das Personalaktengeheimnis Vorrang.

Aufsichtsrechtliche Maßnahmen müssen nach der DS-GVO zur Gewährleistung der Einhaltung des Datenschutzrechts geeignet, erforderlich und verhältnismäßig sein. Ein Bußgeld kam nicht in Betracht: Gegen öffentliche Stellen in Baden-Württemberg dürfen gemäß Artikel 83 Abs. 7 DS-GVO in Verbindung mit § 28 LDSG (Landesdatenschutzgesetz) keine Geldbußen verhängt werden. Im vorliegenden Fall eines einmaligen und nicht mehr andauernden Datenschutzverstoßes durch eine öffentliche Stelle des Landes wäre als einzig mögliche und damit zugleich schwerste Abhilfemaßnahme eine förmliche Verwarnung zulässig gewesen.

Eine Verwarnung gegen öffentliche Stellen ist vorwiegend dann auszusprechen, wenn dies wegen einer Wiederholungsgefahr zur Gewährleistung der Einhaltung des Datenschutzrechts erforderlich ist. Eine Wiederholungsgefahr war hier nach unserer Einschätzung aber nicht anzunehmen. In seiner Stellungnahme uns gegenüber hat das Innenministerium sich unserer rechtlichen Bewertung angeschlossen, dass die Übermittlung des anwaltlichen Schreibens datenschutzrechtlich unzulässig war. Das Innenministerium hat dabei auch die besondere Bedeutung des Personaldatenschutzes anerkannt und den Vorgang zum Anlass genommen, in Kooperation mit uns zu datenschutzrechtlichen Fragen zu sensibilisieren. Eine entsprechende Schulung der Mitarbeitenden des Innenministeriums hat bereits stattgefunden.

Mit Blick auf das zwischenzeitlich abgeschlossene Ermittlungsverfahren gegen Zahlung einer Geldauflage und der politischen Befassung war nicht anzunehmen, dass sich ein solcher Datenschutzverstoß wiederholen wird. Eine förmliche Verwarnung des Innenministeriums war daher nicht erforderlich.

Datenverarbeitung durch den Personalrat

Ein weiteres Thema, das uns im Jahre 2023 beschäftigt hat, war die Datenverarbeitung durch den Personalrat. Die Fragen reichten von der datenschutzrechtlichen Verantwortlichkeit des Personalrats über die Kontrolle des Personalrats durch behördliche Datenschutzbeauftragte bis zur Verarbeitung von Adressdaten bei einer Personalratswahl.

Der Personalrat verarbeitet eine Vielzahl von personenbezogenen Daten. Seine Unabhängigkeit von der Dienststelle macht die datenschutzrechtliche Zuordnung dieser Verarbeitungen und die Datenschutzkontrolle des Personalrats schwierig.

Während die Stellung von Betriebsräten durch die Einführung des § 79a Satz 2 BetrVG zum 18. Juni 2021 geklärt ist, fehlen im LPVG Regelungen zu einer Verantwortlichkeit des Personalrats. Zwar trifft § 67 LPVG Regelungen zu Datenverarbeitungen durch den Personalrat, aus ihm geht jedoch nicht hervor, ob dieser als Verantwortlicher nach Art. 4 Nr. 7 DS-GVO anzusehen ist und ob er der Kontrolle durch behördliche Datenschutzbeauftragte unterliegt oder eine eigene Person als Datenschutzbeauftragte bestellt. Die Formulierung, dass die Personalvertretungen die zur Einhaltung datenschutzrechtlicher Vorschriften erforderlichen ergänzenden Regelungen für ihre Geschäftsführung „in eigener Verantwortung“ treffen, bedeutet nicht, dass sie als Verantwortliche im Sinne des Datenschutzrechts anzusehen sind.

In der Gesetzesbegründung der Vorgängernorm wird der Personalrat als Teil der datenverarbeitenden Stelle bezeichnet, auf den auch die für diese geltenden Kontrollregelungen Anwendung finden (LT-Drs. 11/6312, S. 43). Mithin war nicht beabsichtigt, ihn zur verantwortlichen Stelle im Sinne des Datenschutzrechts zu machen. Damit richtet sich eine Verantwortlichkeit des Personalrats nach Art. 4 Nr. 7 DS-GVO und es kommt darauf an, ob dieser, die Dienststelle oder beide gemeinsam über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet bzw. entscheiden. Mangels Änderung der Sach- oder Rechtslage gehen wir weiterhin davon aus, dass bei der Datenverarbeitung in der Regel keine eigenständige Verwaltung der personenbezogenen Daten durch den Personalrat stattfindet. Gemäß § 2 Satz 1 LPersVG arbeiten die Personalvertretung und die

Dienststelle partnerschaftlich und vertrauensvoll zum Wohl der Beschäftigten und zur Erfüllung der der Dienststelle obliegenden Aufgaben zusammen. Zudem sehen auch die Verwaltungsgerichte den Personalrat eher als Teil der Behörde (dienststellenintern es Organ) denn als selbstständige Größe der Interessenvertretung. Deshalb ist der Personalrat nach hiesiger Auffassung bei Datenverarbeitungen im Rahmen seiner Aufgaben nicht selbst Verantwortlicher nach Art. 4 Nr. 7 DS-GVO, sondern Teil der Dienststelle als verantwortliche Stelle, solange im LPVG nichts anderes bestimmt wird oder sich die Sach- und Rechtslage sonst ändert.

Ob der Personalrat der Kontrolle durch behördliche Datenschutzbeauftragte unterliegt, ist mangels gesetzlicher Regelung nicht abschließend geklärt. Für eine Kontrollbefugnis gegenüber dem Personalrat spricht, dass sich die Aufgaben des behördlichen Datenschutzbeauftragten oder der -beauftragten auf die gesamte öffentliche Stelle erstrecken, zu der auch der Personalrat gehört. Allerdings wird vorgebracht, dass eine Kontrolle durch behördliche Datenschutzbeauftragte der Unabhängigkeit des Personalrats widerspreche, indem die entsprechende arbeitsgerichtliche Rechtsprechung zum Betriebsrat übertragen wird (anders aber LAG Baden-Württemberg Beschluss vom 20. Mai 2022, 12 TaBV 4/21, Rn. 61 mit Hinweis auf die frühere Rechtsprechung des BAG). Hiergegen lässt sich jedoch einwenden, dass behördliche Datenschutzbeauftragte gegenüber der Dienststelle hinsichtlich seiner oder ihrer Tätigkeit weisungsunabhängig und zur Verschwiegenheit verpflichtet ist. Die Kontrolle durch ihn oder sie gefährdet die Personalratsarbeit daher nicht. Zudem fehlt es an einer rechtlichen Grundlage für eine Einschränkung der Kontrollbefugnisse des oder der behördlichen Datenschutzbeauftragten, Art. 39 Abs. 1 Buchst. b DS-GVO normiert eine Überwachungsbefugnis für die gesamte verarbeitende Stelle (Verantwortlicher oder Auftragsverarbeiter) eine Befugnis, hiervon abzuweichen, findet sich in der DS-GVO nicht. Diese genießt als unmittelbar anwendbares Unionsrecht Anwendungsvorrang. Die Argumente sprechen daher dafür, dass der Personalrat der Kontrolle des oder der behördlichen Datenschutzbeauftragten unterliegt. Auch die Pflicht des Personalrats zur Verschwiegenheit nach § 7 LPVG steht der Kontrolle durch den die Datenschutzbeauftragten oder -beauftragte nicht entgegen. Es stellt sich bereits die, nicht geklärte, Frage, ob eine erforderliche Weitergabe von Angelegenheiten und Tatsachen an die Datenschutzbeauftragten im Rahmen von deren Kontrollbefugnissen gegenüber dem Personalrat überhaupt gegen die Pflicht, „Verschwiegenheit zu bewahren", verstößt, da sie zu den Aufgaben des Personalrats gehört. Hiergegen spricht, dass kein Offenbaren im Sinne des § 203 Abs. 2 Satz 1 Nr. 3 StGB vorliegt, wenn innerhalb einer Behörde oder Funktionseinheit Mitarbeitenden (hier: dem oder der Datenschutzbeauftragten) im Rahmen ihrer Befugnisse fremde Geheimnisse bekanntgegeben werden. Eine ordnungsgemäße Aufgabenerfüllung als Pflichtverstoß anzusehen sowie personalvertretungsrechtliche und strafrechtliche Verschwiegenheitspflicht auseinanderfallen zu lassen, dürfte vom Landesgesetzgeber mit § 7 LPVG nicht beabsichtigt gewesen sein.

Die Kontrolle muss so ausgestaltet werden, dass kein Verstoß gegen § 7 Abs. 1 Satz 1 LPVG vorliegt. Behördliche Datenschutzbeauftragte sollten der Überwachungs- und Beratungsaufgabe möglichst ohne die Nutzung personenbezogener Beschäftigtendaten nachkommen, etwa indem der Personalrat Fragestellungen in abstrakter Form – also ohne konkreten Einzelfallbezug – an sie richtet. Außerdem sollten sie die Einhaltung technischer und organisatorischer Datenschutzanforderungen durch den Personalrat nach Möglichkeit ohne Kenntnisnahme personenbezogener Beschäftigtendaten überprüfen.

Nach § 67 Abs. 1 Satz 1 LPVG haben die Personalvertretungen bei der Verarbeitung personenbezogener Daten die datenschutzrechtlichen Vorschriften zu beachten und treffen die zu deren Einhaltung erforderlichen ergänzenden Regelungen für ihre Geschäftsführung in eigener Verantwortung. Bereits aus Art. 6 Abs. 1 Unterabs. 1 DS-GVO und § 15 Abs. 1 Satz 2 LDSG folgt, dass der Personalrat personenbezogene Daten nur verarbeiten darf, wenn dies zur Ausübung seiner Rechte und Pflichten erforderlich ist. Damit dürfen im Zusammenhang mit einer Personalratswahl nur die personenbezogenen Daten der Wahlberechtigten verarbeitet

werden, die notwendig sind, um die Wahl entsprechend den Vorgaben des LPVG und der Wahlordnung durchführen zu können. Die Verarbeitung der Privatadressen der Wahlberechtigten ist nur erforderlich, wenn die Verwendung der dienstlichen Adresse für die Organisation der Wahl nicht ausreicht.

Dienststellen sollten sich ihrer datenschutzrechtlichen Verantwortlichkeit für die Datenverarbeitungen der Personalvertretung bewusst sein und dieser die für die Einhaltung des Datenschutzes notwendigen Ressourcen, wie z. B. Schulungen, zur Verfügung stellen. Hier kann bzw. muss auch der oder die behördliche Datenschutzbeauftragte tätig werden.

Zugriff auf Personaldaten und das IT-Grundschutzkompendium des Bundesamts für Sicherheit in der Informationstechnik

Personenbezogene Daten der Beschäftigten müssen nicht nur vor Zugriff durch Außenstehende, sondern auch vor Zugriff durch Mitarbeitende, die sie nicht benötigen, geschützt werden. Dies führt häufig zu Problemen.

Im Laufe des Jahres 2023 haben wir uns wiederholt mit der mangelhaften Sicherung von Personaldaten vor dem Zugriff durch unbefugte Mitarbeitende beschäftigten müssen. Die personenbezogenen Daten der Beschäftigten wurden entweder bewusst in einer Form gespeichert bzw. intern veröffentlicht, dass unberechtigte Mitarbeitende auf diese Zugriff nehmen konnten, oder Zugriffsmöglichkeiten wurden fahrlässig fehlerhaft eingerichtet und nicht im erforderlichen Maße beschränkt.

Nachdem entsprechendes Verhalten im Berichtszeitraum in drei Fällen zu Verwarnungen geführt hat und einen beträchtlichen Teil der Datenpannenmeldungen, Beschwerden und Beratungsanfragen im Bereich des Beschäftigtendatenschutzes ausmacht, soll hier noch einmal zusammenfassend dargestellt werden, welche Mitarbeitenden auf Personaldaten zugreifen dürfen und welche Maßnahmen getroffen werden müssen, um unbefugte Zugriffe zu vermeiden.

Personenbezogene Daten müssen nach Art. 5 Abs. 1 Buchst. c DS-GVO dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Grundsatz der Datenminimierung“). Zudem verlangen die in Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlagen für die Datenverarbeitung stets deren Erforderlichkeit. Hieraus folgt nicht nur, dass nicht mehr personenbezogene Daten erhoben werden dürfen, als zur Erreichung des vom Verantwortlichen verfolgten Zweck benötigt werden. Auch die Anzahl der Verarbeitungsvorgänge und die Zahl der verarbeitenden Personen muss auf das zum Erreichen des Zwecks notwendige Maß beschränkt werden. Daraus ergibt sich, dass nur die Beschäftigten auf personenbezogene Daten zugreifen dürfen, die diese zur Erledigung ihrer Aufgaben, und damit zum Erreichen des mit der Datenverarbeitung verfolgten Zwecks, benötigen ("need to know"). Der Verantwortliche muss definieren, welche Rollen es für Tätigkeiten innerhalb von Geschäftsprozessen gibt, und daraus Umfänge von Berechtigungen (z. B. nur lesen/auch schreiben/auch löschen, Zugriff von extern ja/nein, Zugriff nur innerhalb eines Workflows an einem Schritt) ableiten und diese an entsprechende Mitarbeitende, die diese Rollen ausfüllen, zuweisen. Dies bedeutet, dass z. B. nicht das Teammitglied X zum Zugriff auf die Krankmeldungen der Beschäftigten berechtigt wird, sondern die Rolle „Bearbeitung Krankmeldungen Personalabteilung“. Diese Rolle wird dann X zugewiesen. Beispielhaft muss so überlegt werden, welche Mitarbeitende für welche Tätigkeiten, die eine Verarbeitung von bestimmten Personaldaten verlangen, zuständig ist oder sind. Die Kenntnisnahme der Personaldaten durch andere Personen als die zuständige ist mangels Erforderlichkeit eine rechtswidrige Datenverarbeitung. Vor einer solchen Verarbeitung müssen die Daten gem. Art. 5 Abs. 1 Buchst. f DS-GVO durch geeignete technische und organisatorische Maßnahmen („TOM“) angemessen geschützt werden (Grundsatz der „Integrität und Vertraulichkeit“). In diese Richtung weisen auch Art. 24, 25 und 32 DS-GVO.

Nach Art. 32 Abs. 1 DS-GVO treffen der Verantwortliche und der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen gegebenenfalls unter anderem die Fähigkeit ein, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Bei der Frage, welche technischen und organisatorischen Maßnahmen zu treffen sind, hat der Verantwortliche kein Entschließungsermessen, jedoch im Rahmen der Vorgaben der DS-GVO ein Auswahlermessen. Er hat so betreffend der durch die Verarbeitung entstehenden Risiken für die Rechte und Freiheiten betroffener Personen mit risikoadäquaten Maßnahmen ein angemessenes Schutzniveau zu treffen.

Hierbei kann sich der Verantwortliche an etablierten Standards orientieren (z. B. ISO 31000 bezüglich Risikomanagement und Identifikation, Bewertung und Behandlung von Risiken; ISO 27000-Familie bzw. Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für Informationssicherheitsmanagementsysteme). Im BSI-Grundschutzkompendium sind in sogenannten IT-Grundschutz-Bausteinen Ergebnisse von durchgeführten Risikoanalysen für normale Schutzbedarfe beschrieben und entsprechende Anforderungen abgeleitet.

☛ **IT-Grundschutz-Kompendium:**

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#

Mit dem Berechtigungsmanagement beschäftigt sich der Baustein „OPR 4 Identitäts- und Berechtigungsmanagement“. Ziel ist u. a., eine unzureichende Definition von Prozessen beim Identitäts- und Berechtigungsmanagement und eine ungeeignete Verwaltung von Zutritts-, Zugangs- und Zugriffsrechten, die zu einem Wildwuchs in der Rechtevergabe führt, zu vermeiden. Nach den dort aufgeführten Basis-Anforderungen muss geregelt werden, wie Benutzendenkennungen einzurichten und zu löschen sind, jede muss eindeutig einer Person zugeordnet werden können und längere Zeit inaktive Benutzendenkennungen sollten, und nicht benötigte, wie Gastkonten, müssen deaktiviert bzw. gelöscht werden. Benutzendenkennungen und Berechtigungen und Zutrittsberechtigungen und -mittel dürfen nur aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden (Prinzip der geringsten Berechtigungen, Least-Privilege, und Erforderlichkeitsprinzip, need-to-know). Alle Berechtigungen müssen über separate administrative Rollen eingerichtet werden. Bei personellen Veränderungen müssen die nicht mehr benötigten Benutzendenkennungen und Berechtigungen entfernt und Zugriffs- und Zutrittsberechtigungen und -mittel entzogen bzw. gesperrt werden. Beantragen Mitarbeitende Berechtigungen, die über den Standard hinausgehen, dürfen diese nur nach zusätzlicher Begründung und Prüfung vergeben werden. Es ist zu dokumentieren, welche Mitarbeitenden über welche Berechtigungen und Zutrittsmittel verfügen.

Die entsprechenden Aufzeichnungen sind regelmäßig darauf zu überprüfen, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegeln und ob sie die betrieblichen Anforderungen korrekt abbilden. Der Zugriff auf IT-Systeme und Dienste muss durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzenden, Dienste oder IT-Systeme abgesichert sein, der Passwortgebrauch muss nach den näheren Vorgaben geregelt werden. Die Beschäftigten sollten über den korrekten Umgang mit Zugangsmitteln geschult werden.

Mit den Anforderungen an die Definition der Zuständigkeiten beschäftigt sich der Baustein ORP.2 Personal: Nach den dortigen Basis-Anforderungen müssen die Aufgaben und Zuständigkeiten von

Mitarbeitenden in geeigneter Weise dokumentiert sein. Ihnen muss der rechtliche Rahmen ihrer Tätigkeit bekannt sein. Außerdem müssen alle Mitarbeitenden darauf hingewiesen werden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind. Weiterhin muss es für alle wesentlichen Geschäftsprozesse praktikable Vertretungsregelungen geben und der Aufgabenumfang der Vertretung muss im Vorfeld klar definiert werden.

Wenn ein Verantwortlicher die Anforderungen des BSI bezüglich des Zugangs zu personenbezogenen Daten für den einschlägigen Schutzbedarf erfüllt, ist die Wahrscheinlichkeit hoch, dass unbefugte Zugriffe der Beschäftigten vermieden werden und den datenschutzrechtlichen Pflichten entsprochen wird. So kann die Umsetzung der von Art. 5 Abs. 1 Buchst. f DS-GVO und Art. 32 Abs. 1 DS-GVO verlangten TOM gewährleistet werden und aufsichtsbehördliche Verfahren und Maßnahmen können vermieden werden.

Bild: Andrey Popovstock.adobe.com

Manche Autos wollen mit Kameraüberwachung Sicherheit bieten – und können über das Ziel hinaus schießen.

Mobilität und Datenschutz

Die Mobilität der Zukunft ist datenintensiv. Hochautomatisiertes und autonomes Fahren sind ohne die Verarbeitung großer Datenmengen nicht möglich. Moderne Fußgänger- und Verkehrsleitsysteme basieren auf Bewegungsdaten und -mustern. Eine DS-GVO konforme Datennutzung ist vor allem dann sehr gut möglich, wenn man den Datenschutz früh bei der Technikgestaltung berücksichtigt.

Audiovisuelle Umgebungserfassung im Rahmen von Entwicklungsfahrten

Im vergangenen Tätigkeitsbericht haben wir über den „Drive-Pilot" der Mercedes-Benz AG berichtet, für den der Automobilhersteller als weltweit erster eine international gültige Systemgenehmigung für hochautomatisiertes Fahren (SAE-Level 3) erhalten hat. Im Hinblick auf die Entwicklung derartiger Systeme äußern Automobilhersteller und Zulieferer zunehmend den Bedarf, Entwicklungs- und Erprobungsfahrten unter realen Fahr- und Verkehrsbedingungen durchführen zu können. Diese dienen dazu, sowohl den Nutzungsgrad bestehender oder neu zu entwickelnder Assistenzsysteme, Fahrfunktionen und damit in Kontext stehende Dienste als auch ihre Verwendung zum automatisierten Fahren bis hin zur autonomen Mobilität zu entwickeln und zu verbessern.

Bei der audiovisuellen Umgebungserfassung werden personenbezogene Daten beispielsweise von Verkehrsteilnehmenden und weiteren Personen (z. B. Insassen anderer Fahrzeuge oder Personen, die zu Fuß, mit einem Fahrrad oder Motorrad am Verkehr teilnehmen) und Kfz-Kennzeichen in der räumlichen Umgebung der Fahrzeuge verarbeitet. Da die Einholung von Einwilligungen aller betroffenen Personen nicht möglich erscheint, kommt als Rechtsgrundlage für die Zulässigkeit der Datenverarbeitung im Regelfall nur Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO in Betracht. Danach ist eine Datenverarbeitung rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unter Beteiligung unserer Behörde wurde hierzu ein Positionspapier der Aufsichtsbehörden erarbeitet, das im September 2023 durch die Datenschutzkonferenz verabschiedet wurde. Dabei wurden mit dem Verband der Automobilindustrie e.V. auch mehrere deutsche Automobilhersteller miteinbezogen.

Das Papier legt gleichsam den Grundstein für eine datenschutzrechtliche Bewertung der Erhebung von personenbezogenen Daten in der Umgebung von Test- und Entwicklungsfahrzeugen sowie deren Weiterverarbeitung. Es geht dabei auf die einzelnen Voraussetzungen der Rechtsgrundlage des Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO ein, wobei ein Schwerpunkt auf der vom Verantwortlichen anzustellende Abwägung der Interessen der betroffenen Personen und des Verantwortlichen liegt. Darüber hinaus werden weitere Aspekte wie z. B. Datenschutz durch Technikgestaltung, die Durchführung einer Datenschutz-Folgenabschätzung, Wahrung der Betroffenenrechte, Erfüllung der Informationspflichten, datenschutzrechtliche Verantwortlichkeit und Datenübermittlung behandelt.

☛ DSK-Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten:

datenschutzkonferenz-online.de/media/dskb/DSK_Positionspapier_audiovisuelle_Umgebungserfassung.pdf

Wächtermodus geht auch anders

Der Einsatz von Video-Parkwächtern hat uns im vergangenen Tätigkeitsbericht beschäftigt. Es handelt sich hier um im Fahrzeug fest verbaute Kameras, die dazu eingesetzt werden, die Fahrzeugumgebung zu filmen. Die Kameradaten können algorithmisch

ausgewertet werden mit dem Ziel, Situationen zu erkennen, die eine Gefahr für das abgestellte Fahrzeug darstellen. In solchen Situationen werden sodann Aufzeichnungen der Fahrzeugumgebung angefertigt, die beispielsweise dazu dienen sollen, im Falle einer Sachbeschädigung Beweismaterial zur Verfügung zu haben. Die Kehrseite der Medaille besteht jedoch aus datenschutzrechtlicher Sicht darin, dass bei einer permanenten Erfassung der Umgebung zur Detektion von Gefahrsituationen personenbezogene Daten von Passant_innen verarbeitet werden, die ihrerseits keinerlei Anlass für eine Beobachtung gegeben haben. Dies stellt einen nicht gerechtfertigten Eingriff in das Recht jedes Menschen dar, sich grundsätzlich unbeobachtet im öffentlichen Raum bewegen zu können. Intensiviert wird der Eingriff in Fällen, in denen eine Speicherung von Aufnahmen schon allein deswegen ausgelöst wird, weil sich Personen dem Fahrzeug aus einer bestimmten Richtung nähern, d. h. der Algorithmus eine Gefahrsituation errechnet, die tatsächlich gar nicht besteht.

Ein prominentes Beispiel für einen Video-Parkwächter ist der Sentry-Mode (Wächtermodus) des kalifornischen Automobilherstellers Tesla. Die in Europa für die Unternehmensgruppe zuständige niederländische Aufsichtsbehörde hat zwischenzeitlich in Bezug auf den Sentry-Mode darüber informiert, dass Tesla im Rahmen einer Untersuchung Veränderungen am Sentry-Mode vorgenommen habe, die den Fahrer_innen eine datenschutzkonformere Nutzung ermöglichten. Beispielsweise werde der Sentry-Mode nur dann aktiviert, wenn das Fahrzeug berührt werde, und nicht schon dann, wenn die Kameras eine verdächtige Aktivität in der Fahrzeugumgebung detektieren würden. Darüber hinaus begännen die Kameras nicht automatisch mit dem Filmen, sondern der Eigentümer oder die Eigentümerin erhalte zunächst einen Warnhinweis auf seinem Mobiltelefon. Das Fahrzeug könne immer noch Kameraaufnahmen anfertigen, allerdings nur dann, wenn der Nutzende diese Funktion aktiviere. Wenn die Kamera aufzeichne, werde eine entsprechende Nachricht auf dem Touchscreen im Fahrzeuginneren eingeblendet und die Scheinwerfer würden aufleuchten. Dadurch würden Menschen darüber informiert, dass das Fahrzeug sie möglicherweise aufzeichne. Darüber hinaus werde in der Standardeinstellung nur die letzte Minute der Aufzeichnungen gespeichert, der Eigentümer auf bis zu zehn Minuten erhöhen könne. Letztlich würden die Aufnahmen ausschließlich im Fahrzeug gespeichert werden, wie es bereits bisher der Fall gewesen sei, und könnten nicht mit Tesla geteilt werden.

Da die Nutzer_innen des Tesla Sentry-Mode bei einem im öffentlichen Straßenraum abgestellten Fahrzeug zumindest auch Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO sind, müssen sie weiterhin sorgfältig prüfen, ob die Nutzung der Kamerafunktion im Einzelfall im Hinblick auf die Rechtsgrundlage des Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO zulässig ist, wenn nicht die Voraussetzungen einer anderen Rechtsgrundlage, wie z. B. einer Einwilligung, vorliegen. Nach Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO ist eine Datenverarbeitung rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Ein solches berechtigtes Interesse kann zum Beispiel unter Umständen dann angenommen werden, wenn tatsächlich eine Gefahr für das Fahrzeug droht. Der Nutzer oder die Nutzerin muss diese Gefahrenlage zudem aufgrund der Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO nachweisen können.

Nach unserem bisherigen Kenntnisstand kann nicht davon ausgegangen werden, dass es dafür in jedem Fall ausreicht, dass der Nutzer oder die Nutzerin einen Warnhinweis auf dem eigenen Mobiltelefon erhält. Daneben müssen auch die weiteren datenschutzrechtlichen Anforderungen der DS-GVO an Verantwortliche, wie z. B. Sicherheit der Verarbeitung, die Informationspflichten und die Betroffenenrechte, erfüllt werden. Im Falle eines Verstoßes gegen die DS-GVO müssen Verantwortliche mit aufsichtsrechtlichen Maßnahmen rechnen.

Auch wenn die Änderungen am Sentry-Mode durch Tesla zu begrüßen sind, ist es nicht ausge-

schlossen, dass Nutzer_innen diesen in einer Weise einsetzen, die datenschutzrechtlich nicht zulässig ist. Sie haben es aber in der Hand, beim Einsatz der Technik zu differenzieren und sind gegebenenfalls weiterhin zumindest auch Verantwortliche im Sinne der DS-GVO.

Fußgänger und digitale Wegweiser – erfolgreiche Auswertung von Interaktion

Ein Wegweiser, dessen Pfeile sich drehen, dürfte nach hergebrachtem Verständnis irritierend sein für Stadttouristen. Doch bei den neuen Stelen eines digitalen Fußgängerleitsystems ist dies anders, wie eine durch uns beratene kamerabasierte Untersuchung zeigen konnte.

Zwei von der Stuttgarter Marketing GmbH in der Stuttgarter Innenstadt installierte Stelen eines digitalen Fußgängerleitsystems verfügen über drehbare Pfeile, auf welchen digitale Hinweise auf aktuelle Attraktionen, wie beispielsweise auf eine Opernaufführung am Abend, angebracht sind. Diese Informationen sind wiederum mit weiteren digitalen Informationsquellen über QR-Codes verknüpft und können laufend geändert werden. Diese Neuheit erscheint zunächst einmal sehr fancy und kann ein Hingucker sein – aber lohnt sich der Aufwand auch? Interagieren Passanten tatsächlich mit der neuen Informationsquelle, oder „schlappen" die Leute achselzuckend daran vorbei? Um dies herauszufinden, wurde eine Untersuchung durch das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO in Stuttgart beauftragt. Die dafür notwendige Datenbasis sollte durch eine Passantenbefragung sowie durch eine algorithmusbasierte Auswertung von Kameradaten geschaffen werden.

Im Rahmen der Beratung bezüglich der Anfertigung der Kameraaufnahmen haben wir unter anderem darauf hingewiesen, dass für den Fall, dass die Punktdichte unterhalb von 16 mm/Pixel liegt, regelmäßig davon ausgegangen werden kann, dass kein Personenbezug vorliegt und somit die DS-GVO keine Anwendung findet. Sollte eine höhere Punktdichte gewählt werden, müssen die Voraussetzungen einer Rechtsgrundlage gem. Art. 6 Abs. 1 DS-GVO vorliegen. In Betracht kommt dafür insbesondere Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO. Danach ist eine Datenverarbeitung rechtmäßig, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Im Rahmen der Prüfung der Erforderlichkeit kommt es beispielsweise darauf an, ob eine noch geringere Punktdichte gewählt werden oder die Erhebung auf schwarz/weiß beschränkt werden kann. Darüber hinaus ist eine umfassende Interessenabwägung vorzunehmen und gemäß Art. 5 Abs. 2 DS-GVO zu dokumentieren. Für das Überwiegen der Interessen des Verantwortlichen kann insbesondere sprechen, wenn es sich um eine Verarbeitung zu wissenschaftlichen Forschungszwecken im Sinne von Art. 89 DS-GVO handelt, wenn es sich um eine relativ schlechte Bildqualität und lediglich kurzzeitige Erfassung der betroffenen Personen handelt, d. h. ein geringer Informationsgehalt besteht, und die Verarbeitung nicht auf eine Identifizierung der betroffenen Personen gerichtet ist. Auch die überobligatorische Erfüllung gesetzlicher Pflichten, wie beispielsweise im Hinblick auf die Transparenz, spricht für ein Überwiegen der Interessen des Verantwortlichen. Gemäß Art. 5 Abs. 1 Buchst. e DS-GVO müssen personenbezogene Daten in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.

Im Sommer 2023 wurde die Datenerhebung durchgeführt. Wie uns im Nachgang mitgeteilt wurde, war die auf diese Weise gesammelte Datenbasis trotz erheblich reduzierter Bildqualität bzw. verringerter Pixeldichte und dem Verzicht auf Farben gut genug, um durch eine algorithmische Auswertung aussagekräftige Ergebnisse zu erzielen. Für die Stuttgarter Marketing GmbH dürfte darüber hinaus auch das positive Fazit bezüglich der Interaktion mit den digitalen Stelen erfreulich gewesen sein. Laut des Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO in Stuttgart hätten dank der so

Bild: LfDI BW

Ein neues digitales Leitsystem in der Stuttgarter Innenstadt.

generierten Datenbasis darüber hinaus Empfehlungen für weitere Aufstellungsorte gegeben werden können. Eine dritte Säule sei bereits im Gespräch.

☛ **Mehr zu Videobildauflösung, und die Frage, ob bei einer Videoüberwachung per se personenbezogene Daten erfasst werden: Tätigkeitsbericht Datenschutz 2019, S. 35f. und Anhang S. 124:**

www.baden-wuerttemberg.datenschutz.de/tatigkeitsbericht

Daten für den digitalen Zwilling des Landesverkehrsmodells

Das Verkehrsministerium hat uns im Vorfeld der Erhebung von Kameradaten an Grenzübergängen beratend hinzugezogen.

Für die Erstellung eines digitalen landesweiten Verkehrsmodells (LVM-BW) erhebt das Verkehrsministerium Baden-Württemberg Daten für die bessere Planung, Erforschung und Analyse von Verkehrswegen. Das neue Verkehrsmodell soll einen digitalen Zwilling des aktuellen Verkehrssystems darstellen, mit dessen Hilfe ab 2025 die Mobilität der Zukunft simuliert werden könne. Mit den zusätzlichen Daten sollen Verkehrsströme besser sichtbar und Prognosen für die Zukunft möglich gemacht werden. Beispielsweise soll damit errechnet werden können, wo Bedarf für einen Radschnellweg besteht.

Zu diesem Zweck sollten speziell Daten zu den Verkehrsströmen an der baden-württembergischen Grenze zu Frankreich und über den Korridor Lindau nach Österreich erhoben werden. Neben Befragungen sollten an den Straßen- und Brückengrenzübergängen Kameras für die Verkehrszählungen zum Einsatz kommen. Aufgrund unserer Beratung wurde beim Kameraeinsatz eine geringe Pixeldichte gewählt, bei der keine Verarbeitung personenbezogener Daten stattfindet (vgl. dazu auch den Beitrag „Fußgänger und digitale Weg-

weiser – erfolgreiche Auswertung von Interaktion“ sowie den Tätigkeitsbericht 2019, S.35f. und S. 124). Persönliche Merkmale wie zum Beispiel Gesicht, Geschlecht oder auch Fahrzeug-Kennzeichen können dadurch nicht erkannt werden. Die betroffene Bevölkerung wurde vorab entsprechend informiert.

Eine Datentreuhand für Mobilitätsdaten – ein Modell für die Zukunft?

Die Datentreuhand wird aktuell in unterschiedlicher Gestalt als vielversprechende Möglichkeit zur Nutzung von Daten diskutiert. Ein Projektkonsortium bestehend aus dem FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur, dem Karlsruher Institut für Technologie (KIT) und dem FZI Forschungszentrum Informatik hat uns im Rahmen des Projekts Treuhandstelle für Mobilitätsdaten („TreuMoDa“, www.treumoda.de) beratend hinzugezogen. Im Zentrum steht dabei die Entwicklung eines Konzepts für einen Dienst zur Vermittlung und Anonymisierung von Mobilitätsdaten.

Wie bereits die vorangegangenen Beiträge zeigen, stellen Mobilitätsdaten ein begehrtes Gut dar, dessen Nutzung wirtschaftlich attraktiv sein kann. Ein weiteres Beispiel von interessanten Mobilitätsdaten sind solche, die zunächst im Rahmen eines Forschungsprojekts erhoben wurden, und mit denen auch ein Unternehmen des öffentlichen Personennahverkehrs arbeiten möchte. Naheliegend ist es für ein Verkehrsunternehmen dann etwa, die Daten sozusagen „einzukaufen“. Dies kann insbesondere kostengünstiger sein, als die Datenbasis selbst neu zu schaffen. Enthalten die Mobilitätsdaten auch personenbezogene Daten, ist die Abwicklung eines solchen Geschäfts aber nicht in jedem Falle zulässig. So könnten sich etwa die zuvor im Rahmen des Forschungsprojekts eingeholten Einwilligungen nur auf die Verarbeitung im Rahmen des Forschungsprojekts selbst beziehen. In der Regel ist dann nicht nur die Zulässigkeit der Zweckänderung fraglich, sondern es besteht dann auch weder eine Rechtsgrundlage für die Übermittlung an das Verkehrsunternehmen noch für die Erhebung durch das Verkehrsunternehmen.

Würde man dagegen die Daten zunächst anonymisieren, kann sich dagegen die Rechtslage – je nach den konkreten Umständen im Einzelfall – anders darstellen. Zwar muss auch die mit der Anonymisierung verfolgte Zweckänderung zulässig sein und bedarf selbst einer Rechtsgrundlage. Allerdings kann sich hier die gegebenenfalls erforderliche Interessenabwägung (etwa nach Art. 6 Abs. 4 oder Art, 6 Abs. 1 Buchst. f DS-GVO) anders darstellen als bei der Übermittlung nicht anonymisierter Daten. Für die Übermittlung sowie für die Erhebung bereits anonymisierter Daten bedürfte es keiner Rechtsgrundlage mehr. Denn diese weisen keinen Personenbezug auf und unterfallen damit nicht dem Anwendungsbereich der Datenschutz-Grundverordnung (Art. 2 Abs. 1 DS-GVO).

Die Anonymisierung von Mobilitätsdaten kann jedoch sehr anspruchsvoll sein und möglicherweise nicht im Rahmen eines Forschungsprojekts selbst geleistet werden. Darüber hinaus kann es beispielsweise bei Bilddaten vorkommen, dass zwar, etwa durch eine Verringerung der Pixeldichte, die Anonymisierung erfolgreich durchgeführt wird (vgl. Beitrag „Daten für den digitalen Zwilling des Landesverkehrsmodells“). Je nachdem, wozu die Daten eingesetzt werden sollen, kann die Datenqualität für das Verkehrsunternehmen aber aufgrund der Verpixelung zu schlecht sein, um sie für Zwecke des nachnutzenden Verkehrsunternehmen gebrauchen zu können. Aus Sicht des Verkehrsunternehmens wäre der „Einkauf“ solcher Daten dann wohl als eine Fehlinvestition zu bewerten.

Solche Schwierigkeiten sollen durch die Treuhandstelle überwunden werden. Diese anonymisiert zunächst nur eine Probe der Daten des Datengebers, d. h. in unserem Beispiel eine Probe aus den Daten des Forschungsprojekts. Bestimmt der Datengeber dabei weiterhin die Zwecke und Mittel der Verarbeitung, kann dies im Rahmen eines Auftragsverarbeitungsvertrags gemäß Art. 28 DS-GVO erfolgen. Der Datennehmer, hier das Verkehrsunternehmen, erhält sodann die anonymisierten Probe-Daten, um zu testen, ob er diese für die von ihm vorgesehenen Zwecke verwenden kann. Nur wenn der Datennehmer mit dem Ergebnis zufrieden ist, werden die gesamten angefragten Daten durch

die Datentreuhand anonymisiert und dem Datennehmer kostenpflichtig zur Verfügung gestellt. Das wirtschaftliche Risiko beim Geschäft mit anonymisierten Daten wird dadurch deutlich abgemildert.

Allerdings ist noch der Umstand zu berücksichtigen, dass ein Anonymisierungsverfahren „veralten" kann: Für die Beurteilung der Frage, ob der Personenbezug eines Datums (wieder-)hergestellt werden kann, sind nach dem Erwägungsgrund 26 zur DS-GVO nämlich „die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen" zu berücksichtigen. Soweit aber technologische Entwicklungen zum Zeitpunkt der Verarbeitung noch nicht absehbar waren und infolge dieser technologischen Entwicklungen – beispielsweise durch neuartige Anwendungen Künstlicher Intelligenz – eine Re-Identifikation ermöglicht wird, können zwischenzeitlich als anonym zu betrachtende Daten wieder personenbezogen werden. So ist es zum Beispiel vorstellbar, dass trotz einer derzeit zur Anonymisierung führenden Verpixelung in der Zukunft durch neuartige Technologien die Verpixelung wieder derart rückberechnbar sein wird, dass die ursprünglich abgebildete Person wieder identifizierbar wird. Daher soll auch ein Abonnementdienst angeboten werden, bei dem immer wieder geprüft wird, ob bereits anonymisierte Daten immer noch ohne Personenbezug sind.

Dieser Ansatz für die Gestaltung einer Datentreuhand stellt alles in allem eine interessante Chance für eine DS-GVO-konforme, wirtschaftliche (Mehrfach-)Verwertung von zunächst personenbezogenen Daten dar, die auch neue Entwicklungen im Hinblick auf Re-Identifizierungs- und Anonymisierungsverfahren mit im Blick hat. Die Projektpartner hoffen nun darauf, das erarbeitete Konzept für TreuMoDa tatsächlich umsetzen zu können.

Mangelhafte IT-Sicherheit führt zu zahlreichen Datenschutzverstößen

Die Gewährleistung von IT-Sicherheit ist eine stetige Herausforderung für Unternehmen, Behörden, Vereine und andere öffentliche wie private Stellen. Auch 2023 konnten wir wieder beobachten, dass mangelhafte IT-Sicherheit zu teils gravierenden Datenschutzverstößen, unrechtmäßiger Veröffentlichung von Daten und großen Schäden für betroffene Personen und zahlreiche Verantwortliche führte.

Laut dem Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage zur IT-Sicherheit 2023 so hoch wie nie. Dabei sind laut BSI überproportional häufig Kommunalverwaltungen betroffen, insbesondere bei Ransomware. Diese haben oftmals nicht genügend Personal, verarbeiten aber teils sehr sensible Daten und sollten daher einen größeren Stellenwert auf IT-Sicherheit legen, um solche Risiken frühzeitig zu vermeiden.

☛ **Lagebericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage zur IT-Sicherheit 2023:**

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7

Auch wir erhielten 2023 beinahe täglich Meldungen über Ransomware-Vorfälle von Unternehmen und Behörden unterschiedlicher Größen. Da mit solchen Fällen in aller Regel ein Risiko einhergeht,dass die Rechte und Freiheiten der betroffenen Personen verletzt wurden oder werden können, sind diese nach Artikel 33 DS-GVO meldepflichtig.

Eine wichtige Frage für Verantwortliche ist, wann die betroffenen Personen über den Verlust des Schutzes personenbezogener Daten nach Artikel 34 DS-GVO informiert werden müssen. Dies ist dann der Fall, wenn der Vorfall voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Der Europäische Datenschutzausschuss hat zwei Hilfestellungen für diese Frage veröffentlicht:

- Die „Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten: edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_de
- Die „Guidelines 9/2022 on personal data breach notification under GDPR“ (derzeit nur in englischer Sprache erhältlich: edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

Demnach ist bei Ransomware-Vorfällen in der Regel eine Information der Betroffenen erforderlich, insbesondere wenn Artikel-9-Daten betroffen sind, Exfiltration von Daten stattgefunden hat, wenn Daten von einem Server oder dem Computer einer Person unberechtigt kopiert, übertragen oder abgerufen werden, oder diese gar veröffentlicht wurden.

Phishing und neue Betrugs-Maschen

Häufig sind zudem auch Phishing-Angriffe auf Nutzende von Cloud-Diensten aller Art, insbesondere Online-Speicher und E-Mail-Dienste. Die Gefährlichkeit von Phishing wird häufig unterschätzt, da oftmals nicht klar ist, auf welche Daten die Angreifer zugegriffen haben und kompromittierte E-Mail-Konten vermeintlich nur zum Verschicken von Spam und Malware verwendet werden. Aber gerade davon kann bei den Empfänger_innen ein hohes Risiko ausgehen, da Malware zahlreiche Folgeschäden verursachen kann und aufgrund vermeintlich vertrauenswürdiger Absender_innen oftmals nicht oder zu spät als Schadsoftware erkannt wird.

Angriffe auf E-Mail-Konten bringen seit einiger Zeit aber auch noch ein weiteres Risiko mit sich: Angreifer_innen durchsuchen die Ein- oder Ausgangsmails nach kürzlich verschickten Rechnungen, ändern die Kontonummer der Empfänger_innen und verschicken die Rechnung erneut. Wenn die Angreifer_innen die Kontrolle über das Empfänger-Postfach haben, löschen sie die ursprüngliche Rechnung. Wenn sie nur die Kontrolle über den Absender haben, geben sie vor, eine Aktualisierung zu verschicken. Durch diese Masche entsteht oftmals ein hoher finanzieller Schaden, zumal die fehlgeleitete Überweisung meistens erst zu spät entdeckt wird.

Verantwortliche sollten daher nach erfolgreichen Phishing-Vorfällen genau prüfen, auf welche E-Mails (potenziell) zugegriffen wurde, welche E-Mails verschickt wurden und ob Umleitungen eingerichtet wurden, mit denen die Angreifer_innen sich dauerhaft Kopien aller Eingangsmails weiterleiten lassen. Neben der Pflicht, bei hohem Risiko nach Artikel 34 DS-GVO die Betroffenen zu informieren, kann es auch zum Schutz vor zivilrechtlichen Schadensersatzforderungen sinnvoll sein, Geschäftspartner_innen und andere Betroffene zu informieren.

Wichtiger ist aber, solche Vorfälle bereits im Vorfeld zu erschweren:

- 2-Faktor-Authentifizierung erschwert Angreifern den Zugang zu fremden Cloud-Konten. Dieser Schutz ist sehr sinnvoll, allerdings beobachten wir immer mehr, dass dieser Schutz umgangen wird, er kann daher nicht als alleinige Maßnahme ausreichen.
- Die Nutzung von Cloud-Diensten sollte so eingeschränkt werden, dass nur berechtigte Personen Zugriff haben. Einen guten Schutz bieten beispielsweise individuelle Client-Zertifikate oder die Beschränkung des Zugriffs auf den vom Verantwortlichen genutzten IP-Address-Bereich.
- Beschäftigte sollten regelmäßig für Phishing-Gefahren sensibilisiert werden.

Sicherheitslücken bei Webseiten und Online-Diensten

Wir haben 2023 mehrere Hinweise auf Sicherheitslücken bei Internetangeboten von Unternehmen aus verschiedenen Branchen und Behörden erhalten, die zur Offenlegung großer Datenmengen geführt haben. Teilweise haben die Verantwortlichen zuvor auf Hinweise nicht reagiert. Anders als

Betrugsmaschen zu erkennen ist nicht immer leicht, deshalb ist Vorsicht geboten.

private Hinweisgeber_innen haben wir als Datenschutz-Aufsichtsbehörde nach Artikel 58 DS-GVO die Möglichkeit, in solchen Fällen die Verantwortlichen anzuweisen, die Sicherheitslücke schnell zu schließen oder, wenn dies nicht möglich ist, gar den jeweiligen Dienst vorläufig zu stoppen, dadurch die Gefahrenquelle zu beseitigen und so dafür zu sorgen, dass das Risiko für betroffene Personen reduziert wird. Üblicherweise schließen Verantwortliche nach unseren Hinweisen und Anhörungen solche Lücken schnell, so dass eine förmliche Anordnung unterbleiben kann.

Ursachen für solche Sicherheitslücken sind in aller Regel Fehler bei der Software-Entwicklung oder der Server-Konfiguration, die von aufmerksamen Fachleuten schnell bemerkt würden. Häufige Ursachen sind zum Beispiel:

- Offen einsehbare Debug-Werkzeuge (wie Symfony Profiler), wodurch Login-Daten für Admins und Datenbanken veröffentlicht werden. Mit diesen Daten können Angreifer_innen sich bei der jeweiligen Anwendung oder gar direkt bei der Datenbank anmelden und so umfangreiche Daten abgreifen. Solche Werkzeuge sollten ausschließlich in der Entwicklung genutzt werden. Ist ausnahmsweise eine Nutzung in Produktion notwendig, muss der Zugang gut abgesichert werden.
- Online verfügbare Rechnungen, Kunden-Uploads oder sonstige Dokumente, die von der Software mit fortlaufenden Nummern im Dateinamen versehen werden, wodurch es sehr leicht ist, auf fremde Daten anderer Nutzer zuzugreifen. Angreifer_innen können damit viele Daten kopieren und entsprechende Zugriffe werden meist nicht entdeckt. Wenn Dateien öffentlich ohne weitere Authentisierung zugänglich sein müssen, sollten die Dateinamen ausreichend lange Zeichenketten aus Zufallswerten (z. B. eine UUID Version 4 nach RFC 4122) enthalten.
- Immer wieder gibt es auch offen im Netz zugängliche Datenbanken mit Standard-Passwörtern oder solchen, die leicht erratbar sind.

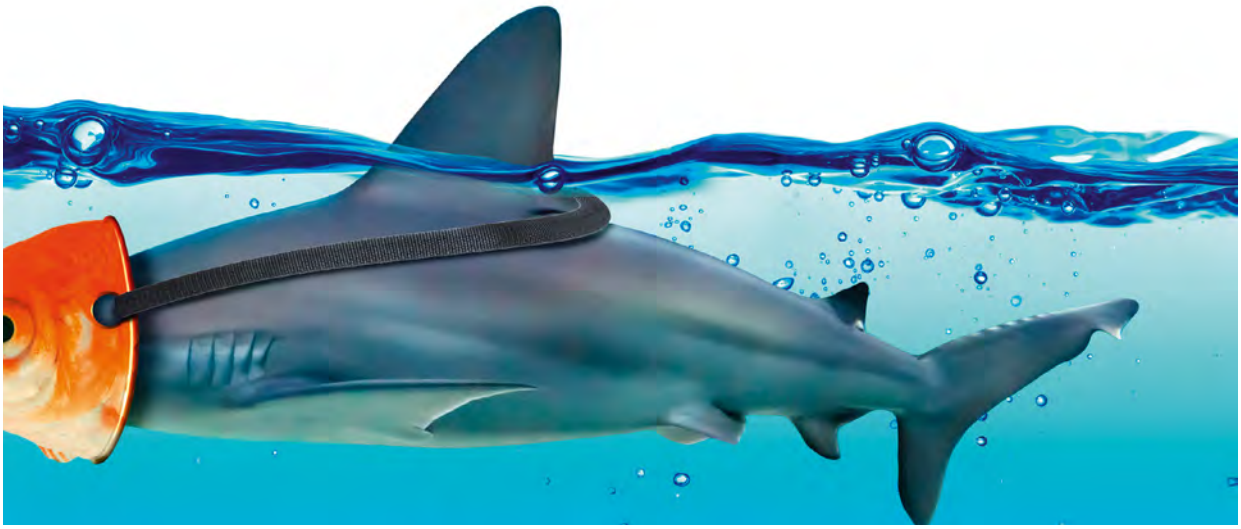


Bild: Romolo Tavani-stock.adobe.com

- Viele Web-Entwickler_innen nutzen heutzutage Schnittstellen von Drittanbietern und greifen auf diese mittels API-Keys zu. Wenn diese im Quelltext einer Webseite zu finden sind oder anderweitig an die Nutzenden gelangen, können sie dort von jedem ausgelesen und verwendet werden, um auf die Schnittstelle direkt zuzugreifen und Daten auszulesen.

Das Open Worldwide Application Security Project (OWASP) veröffentlicht seit 2003 eine Liste der zehn häufigsten Sicherheitsrisiken bei Web-Applikationen. Web-Entwickler_innen sollten ihre Anwendungen regelmäßig auf diese Risiken prüfen und Verantwortliche eine solche Prüfung von ihren Auftragnehmern einfordern. Je nach Größe des Projekts oder Risikos bietet es sich auch an, unabhängige professionelle Audits durchführen zu lassen oder die Anwendung selbst z. B. anhand des OWASP Web Security Testing Guide zu prüfen. Verantwortliche müssen IT-Sicherheit stärker und frühzeitig beachten, um den Anforderungen des Datenschutzes gerecht zu werden. Dies gilt sowohl bei Eigenentwicklungen als auch bei der Vergabe von Aufträgen, bei denen sie sicherstellen müssen, dass sie die einzelnen Dienstleister und sonstigen am Gesamtprojekt Beteiligten wirksam und technisch fundiert kontrollieren können. Insbesondere Behörden und große Unternehmen müssen daher geeignetes internes Personal haben, um im jeweiligen Projektverlauf in der Lage zu sein, ständig den Herausforderungen an die Qualität der Leistungen im Bereich der IT-Sicherheit und des Datenschutzes gerecht zu werden. Eventuelle Mängel können so frühzeitig aufgespürt und behoben werden. Zudem ist es oftmals nötig, eventuelle gegenläufige Interessen der Dienstleister erkennen zu können.

Zwar werden externe Dienstleister oftmals gerne eingesetzt, um die Verantwortung auf mehrere Schultern zu verteilen. Dies entbindet den in der Regel datenschutzrechtlich verantwortlichen Auftraggeber allerdings nicht vor seiner Gesamtverantwortung (vgl. auch Urteil des EuGH, vom 5. Dezember 2023, Az. C-683/21, Randnummer 84f.) und von der Notwendigkeit, eigene interne Kompetenzen aufzubauen. Eine effektive Kontrolle von externen Dienstleistern ist in der Regel dann möglich, wenn interne Mitarbeitende in der Lage wären, mit entsprechendem Zeitaufwand die Dienstleistung selbst zu erbringen.

☛ Mehr Infos

Liste der zehn häufigsten Sicherheitsrisiken bei Web-Applikationen:
owasp.org/www-project-top-ten

OWASP Web Security Testing Guide:
owasp.org/www-project-web-security-testing-guide

EuGH, Urteil vom 5. Dezember 2023:
curia.europa.eu/juris/document/document.jsf?text=&docid=280324&pageIndex=0&doclang=DE&mode=lst&dir=&occ=first&part=1&cid=1043306

Digitale Bildungsplattform und Software für die Schulverwaltung

Wie in den vergangenen Jahren haben wir auch im Berichtsjahr wieder das Ministerium für Kultus, Jugend und Sport bei seinem Vorhaben zur Digitalen Bildungsplattform intensiv unterstützt. Wir nahmen auch weiterhin an den regelmäßigen Sitzungen des Lenkungskreises teil. Aus unserer Sicht hat sich diese Art der Zusammenarbeit sehr bewährt, und es konnten sowohl die IT-Sicherheit als auch der Datenschutz in den Anwendungen der Bildungsplattform gestärkt werden.

Dieses Jahr haben wir uns außerdem ausführlich mit der Ausschreibung des Ministeriums zum neuen Provider für das Lernmanagementsystem Moodle beschäftigt. Wir waren Teil der Kommission im Vergabeverfahren, so dass auf diese Weise unsere datenschutzrechtlichen Hinweise gewürdigt werden konnten. Die Konfiguration von Moodle selbst und die verwendeten Module waren vom Ministerium vorgegeben. Es war möglich, wichtige Hinweise zur IT-Sicherheit und zum Datenschutz direkt in die Vergabeverhandlungen einzubringen und Impulse für Verbesserungen zu geben. Wir sind zuversichtlich, dass der Gewinner der Ausschreibung den Schulen in Baden-Württemberg ein sicheres und datenschutzkonformes Moodle anbieten wird, das den Schulen im Jahr 2024 zur Verfügung stehen wird.

Neben Moodle bietet das Ministerium den Schulen mit itslearning ein weiteres Lernmanagementsystem im Rahmen der Bildungsplattform an. Wie bereits in den letzten Tätigkeitsberichten angesprochen, sehen wir leider immer noch im Bereich des Drittstaatentransfers, des Trackings und der technisch und organisatorischen Maßnahmen Handlungsbedarf. Dazu befinden wir uns weiter mit dem Kultusministerium im Gespräch. Wir hoffen, dass die Fragen hierzu gelöst werden können.

Zentrale Komponente der Bildungsplattform wird das Identitäts- und Access- Management (IdAM) sein. Darüber melden sich die Nutzenden der Bildungsplattform an und haben dann direkt Zugang zu allen weiteren Komponenten, welche die Schule nutzen möchte (Single-Sign-On). Entsprechend muss dieses System sicher gestaltet sein. Auch hier sind wir in die Verhandlungsrunden der Ausschreibung des Ministeriums zur IT-Sicherheit und zum Datenschutz eingebunden. Wir sind zuversichtlich, dass dieses System 2024 den Schulen als zentraler Zugang zur Bildungsplattform zur Verfügung stehen wird.

Wie im vergangenen Tätigkeitsbericht angesprochen, sollen Lehrkräfte einen digitalen Arbeitsplatz mit Textverarbeitung, Tabellenkalkulation und Präsentationssoftware mit Online-Speicher und E-Mail sowie Kalender und Kontakte erhalten. Dazu soll die dPhoenixSuite des Anbieters Dataport verwendet werden, eines Informations- und Kommunikationsdienstleisters für die öffentlichen Verwaltung. Auch hierzu sind wir weiterhin mit dem Kultusministerium im Gespräch.

So erfreulich sich die Zusammenarbeit in Bezug auf die Bildungsplattform mit dem Ministerium gestaltet, hoffen wir auch bei einem davon unabhängigen Thema, dem Schulverwaltungsprogramm ASV-BW, wo noch nicht alle datenschutzrechtliche Fragen geklärt sind, den konstruktiven Austausch fortführen zu können, sodass auch dieser Dienst datenschutzkonform angeboten werden kann.

Bildungszentrum – vielfältiges Bildungsangebot

Wie in den vorausgegangenen Jahren gab es im Bildungszentrum auch im Jahr 2023 eine Vielzahl von Veranstaltungen zu den unterschiedlichen Themen und für verschiedene Zielgruppen wie Behörden, Unternehmen, Initiativen, Vereine und allen interessierten Bürger_innen. Insgesamt konnten rund 120 Veranstaltungen durchgeführt werden, zu denen es über 3.700 Anmeldungen gab. Zudem unterstützen unsere Medienfachleute unsere Dienststelle beispielsweise bei Videoproduktionen, sie haben auch etwa die jährliche KI-Woche technisch begleitet, was sehr umfangreich und anspruchsvoll war.

Im Veranstaltungsbereich wurden unter anderem grundlegende Datenschutzschulungen für öffentliche Stellen, Vereine, für Forschende, zum Sozialdatenschutz, zum Datenpannenmanagement oder der Funktionsweise von KI durchgeführt. Interessierte Bürger_innen konnten bei uns mehr darüber erfahren, wie man einen PC durch Browserwahl- und -einstellung sowie Passwortmanagement fit und sicherer machen kann oder wie Webseitenbetreibende durch täuschende Designpraktiken versuchen, Entscheidungen von Nutzenden in ihrem Interesse zu lenken.

BvD-Herbstkonferenz und Behördentag 2023

In Berichtsjahr fand die alljährliche Herbstkonferenz mit Behördentag des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. unter dem Titel „Next Level Privacy: Fit für die Zukunft" vom 18. bis 20. Oktober 2023 in Aschheim bei München statt. Damit wurde die inzwischen etablierte Kooperation zwischen uns und dem BvD, dem Bayerischen Landesamt für Datenaufsicht und dem Bayerischen Landesbeauftragten für Datenschutz fortgeführt, die Dr. Stefan Brink ins Leben gerufen hat und die engagiert weitergeführt wird. Im Mittelpunkt standen in diesem Jahr im Besonderen Vorträge zu europäischen Rechtsakten, Herausforderungen von und für KI-Technologien in Bezug auf datenschutzrechtliche Fragen und technisches Verständnis von KI-Anwendungen und Datensicherheit, wozu auch die Landesbeauftragte für Datenschutz Schleswig-Holstein Dr. h.c. Marit Hansen als Referentin begrüßt werden konnte.

13 Mitarbeitende von uns reicherten die Veranstaltung durch Fachvorträge an und diskutierten mit den rund 300 anwesenden Fachleuten aus Wirtschaft und öffentlichen Einrichtungen zu aktuellen Fragestellungen. Mit besonderem Interesse wurden auch die Vorträge von Benjamin Brake (Leiter der Abteilung Digital- und Datenpolitik im Bundesministerium für Digitales und Verkehr) sowie von Stefan Sobotta (Referatsleiter Referat V II 4 – Datenschutzrecht im Bundesministerium des Innern für Bau und Heimat) zum Thema „Aktuelle Entwicklungen um DS-GVO und BDSG" verfolgt, die als richtungsweisend kritisch diskutiert wurden.

Wie in jedem Jahr wurde auch die Möglichkeit der „Fragen an die Aufsichtsbehörden" vom Publikum besonders goutiert, bei der die Anwesenden ihre Fragen direkt an die Dienststellenleiter stellen können. Besonders zum Abschluss des Behördentags wurde diese Gelegenheit ausgiebig genutzt und führte zu einem gewinnbringenden Erfahrungsaustausch. Im kommenden Jahr wird die Herbstkonferenz vom 16. bis 18.10. wieder in Stuttgart stattfinden.

Nachfrage nach individuell vereinbarten Veranstaltungen

Es freut uns, dass die Nachfrage nach individuell vereinbarten Veranstaltungen stetig ansteigt. In der Regel werden hierbei Grundlagenschulungen angefragt, aber auch vertiefendende Schulungen zu bestimmten Aspekten des Datenschutzes. Doch nicht alle angefragten Themen konnten und können von uns abgedeckt werden. Teilweise handelt

Bild: LfDI BW

Der Leiter des Bildungszentrums BIDIB Frank Feucht (links) und Martin Rost vom Unabhängigen Landeszentrum für Datenschutz Schleswig Holstein bei einer BIDIB Schulung zum Standard-Datenschutzmodell.

es sich bei den gewünschten Informationen um (komplexere) Einzelfallberatungen. Beratungen in Einzelfallen erfolgen durch den jeweils zuständigen Fachbereich in unserer Behörde, wir liefern strukturelle Beratungen. Natürlich gehen wir auch in Fragenrunden, die es oftmals im Anschluss an die Veranstaltungen gibt, auf einzelne und konkrete Fragen ein. Aber manche Fragen lassen sich nur durch eine konkrete Einzelfallberatung durch unsere Fachrefrent_innen klären.

Teilweise sind angefragte Themen und Fragestellungen auch so aktuell, dass diese noch nicht abschließend diskutiert und entschieden sind, vor allem auf Ebene der deutschen und europäischen Datenschutzgremien. Solche Anfragen entziehen sich somit Schulungen, zumindest soweit diese auf die aktuelle Rechtslage und konkrete Anwendungsfälle in der Praxis abstellen. Und zu guter Letzt sind wir Opfer unseres Erfolges und kommen zunehmend an Kapazitätsgrenzen, da unsere Referent_innen nicht beliebig oft eine Schulung, die vorbereitet werden will, anbieten können, da sie in ihren Fachbereichen viel zu leisten haben.

Schule digital

Wie bereits im vergangenen Tätigkeitsbericht ausgeführt, haben wir das Projekt „Schule digital" initiiert, um den Datenschutz an den Schulen zu stärken, insbesondere durch Fortbildungen für alle am Schulleben Beteiligte – Schulleitungen, Lehrkräfte, Sekretariate an den Schulen, Eltern, Schüler_innen und andere mehr. Dankenswerterweise hat der Landtag uns für diese wichtige Arbeit drei zusätzliche Stellen für den Zeitraum bis Ende 2024 bewilligt.

Im Jahr 2023 wurden bis Ende Dezember über 1.500 Teilnehmende in 80 Veranstaltungen im Projekt „Schule digital" erreicht. Das Projekt ist erfolgreich und sinnvoll.

In Zusammenarbeit zwischen dem Zentrum für Schulqualität und Lehrerbildung (ZSL) haben wir begonnen, die Unterlagen der amtlichen Lehrerfortbildung zum Thema Datenschutz zu überarbeiten. So können nun mit uns abgestimmte Unterlagen zum Datenschutz in der Lehrerfortbildung verwendet werden. Das ZSL hat die Grund-

lagen-Fortbildungen für Schulleitungen und Lehrkräfte zum Datenschutz in Gänze übernommen.

Die dadurch freigewordenen Ressourcen bei uns haben wir genutzt, um vertiefte Datenschutz-Fortbildungen zu spezifischen Themen anzubieten. Neben den Fortbildungen für Eltern, Sekretariaten an Schulen und Datenschutz bei der Kooperation zwischen Kindertageseinrichtung und Grundschule, welche wir weiterhin anbieten, sind nun auch Fortbildungen zu den Themen „technisch-organisatorische Maßnahmen für Schulleitungen", „Datenschutz beim elektronischen Tagebuch", „Datenpannen im Schulbereich", „Datenschutz bei der Nutzung privater Endgeräte im Schuldienst" und „Datenschutz bei Schulwebseiten" im Angebot von Schule digital und können online über das BIDIB gebucht werden. Außerdem haben wir auch den Regierungspräsidien – Abteilung Schule – und einigen Staatlichen Schulämtern die Unterlagen und das Projekt vorgestellt, damit sich diese ein Bild von den Fortbildungen machen konnten. Auf diese Weise wurde die Zusammenarbeit mit diesen Stellen intensiviert.

☛ **Fortbildungsreihe Schule digital**

lfdi-bw.de/schule-digital

Fortbildungen für Verantwortliche in Vereinen

2023 haben unsere Kolleg_innen aus der Abteilung Privatwirtschaft, die auch andere nicht-öffentliche Stellen wie Vereine begleiten, in insgesamt drei Veranstaltungen über 160 Teilnehmer_innen im Hinblick auf die Grundlagen des Datenschutzes in der Vereinsarbeit geschult. Hierbei wurden die Grundbegriffe der DS-GVO und insbesondere die Rechtsgrundlagen der Datenverarbeitung im Verein sowie zahlreiche Schwerpunktthemen wie beispielsweise die vereinsinterne Kommunikation, Löschkonzeptionen und Öffentlichkeitsarbeit sowie nicht zuletzt die Informationspflichten und Datenschutzhinweise in der Vereinspraxis beleuchtet, so dass viele Praxisfragen beantwortet werden konnten.

Medienbereich und Bildungsportal

Auch im Jahr 2023 war der Medienbereich im Bildungszentrum wieder stark in Bewegung. Seit Gründung des Bildungszentrums konzentriert sich der Medienbereich auf die Entwicklung innovativer digitaler Bildungsformate. Durch inzwischen vorhandene Medientechnikausstattung ist die Grundlage für Produktionen im Haus gelegt. Wir wollen die Ausstattung sukzessive erweitern.

Was uns besonders freut: Wir erreichen Bürger_innen sowie Entscheidungsträger_innen gleichermaßen. Unser Ziel ist es, das umfangreiche Wissen, das hier im Haus vorhanden ist, so leicht zugänglich und ansprechend wie möglich zu präsentieren. Im Jahr 2024 wollen wir diesen Weg fortsetzen und weitere innovative Wege finden, um Bildung und Information noch einfacher zugänglich für alle Interessierten zu machen.

Das geplante digitale Bildungsportal soll als Hauptinstrument für diese Entwicklung dienen, welches den Schulungsbereich des Bildungszentrums wirksam stärken soll. Ziel ist es, dass auf dem Bildungsportal Informationen bereitgestellt werden, die Interessierte dann abrufen können, wenn sie es möchten. Somit können sie etwa Grundlagenschulungen auch dann nutzen, wenn es terminlich mit einer Schulung bei uns im Haus nicht passt. Durch Vertiefungsschulungen bei unseren Referent_innen etwa können sie anschließend ihr Wissen erweitern und in Frage- und Diskussionsrunden mit unseren Fachleuten ins Gespräch kommen.

Im Laufe der Zeit haben wir eine Fülle an Erfahrungen gesammelt, die uns im Bildungszentrum sicherer und kreativer im Umgang mit digitalen Medien gemacht haben. Mache Ideen bleiben Ideen, da wir zeitlich nicht alles umsetzen können. Im digitalen Zeitalter sind Medienproduktionen nicht wegzudenken, hybride Veranstaltungen notwendig und ein Angebot wie im Bildungsportal wichtig, um Interessierte über den Datenschutz und die Informationsfreiheit zu informieren.

Projektmanagement

Projektarbeit in unserer Dienststelle

Vor inzwischen drei Jahren wurde das Thema „Projektmanagement“ bei uns gezielt in den Blick genommen und professionalisiert, um dem Trend entgegenzuwirken, dass Projekte engagierter Mitarbeitender, die über die Beschwerde- und Datenpannenbearbeitung hinausgehen, durch das erhöhte Arbeitsaufkommen „versanden“. Hierdurch konnten im Besonderen kreative, interaktive und bürgernahe Projekte vorangetrieben, aber auch intern-organisatorische Themen angegangen werden, um Eingaben effizienter abarbeiten zu können oder trotz Arbeitslast weiterhin ein gutes Arbeitsklima für die Mitarbeitenden zu erhalten.

So wurde im Sommer 2023 ein Projekt neu aufgesetzt, dass die Bedarfe von Start-ups in Baden-Württemberg im Bereich des Datenschutzes in den Blick nimmt und dauerhaft Strukturen und Hilfestellungen schaffen möchte, Start-ups bei datenschutzrechtlichen Fragestellungen auf sichere Beine zu stellen. Hierzu führen wir Gespräche mit verschiedenen externen Multiplikatoren und Stakeholdern, um die Angebote zielgruppengerecht zuschneiden zu können. Erste Ergebnisse sollen im kommenden Jahr präsentiert werden.

Auch öffentlichkeitswirksame Veranstaltungen wie die Lange Nacht der Museen, die BvD-Herbstkonferenz oder Sonderveranstaltungen wie die Diskussionsrunde „Die Zukunft des Datenschutzes – Ist die DS-GVO bereit für KI?“ wird von den Projektmanagement-Beauftragten federführend geplant, koordiniert und begleitet, genauso wie hausinterne Veranstaltungen beispielsweise der Gesundheitstag.

Um die hohe Anzahl an Beschwerden bei gleichbleibender Qualität schneller bearbeiten zu können und gleichzeitig Arbeitsprozesse noch stärker zu vereinheitlichen, wurde eine Projektgruppe damit beauftragt, Arbeitsprozesse der Fachabteilungen in den Blick zu nehmen. Sie soll prüfen, an welcher Stelle man Prozesse optimieren kann, um sowohl die Arbeitslast der Mitarbeitenden durch effizientere Abläufe verringern zu können als auch in der Folge schnellere Rückmeldung an Beschwerdeführer_innen oder Verantwortliche zu ermöglichen. Die Ergebnisse sollen zu Prozessoptimierungen und -vereinheitlichungen führen, die auch neuen Mitarbeitenden die Einarbeitung erleichtert. Im Zuge des Projekts wird ebenso das Online-Beschwerdeformular erneut geprüft, um Rückfragen an Beschwerdeführer_innen gegebenenfalls minimieren zu können und den Bearbeitungsprozess zu beschleunigen. Ebenso findet innerhalb dieses Projekts die Anforderung der leichten Sprache weitergehend Umsetzung in unseren behördlichen Schreiben an Bürger_innen.

Lange Nacht der Museen 2023

Nach dem erfolgreichen Auftakt im Jahr 2022 waren wir im Folgejahr wieder mit dabei – bei der Langen Nacht der Museen (LNM) Stuttgart. Am 25. Märt 2023 öffnete auch die Behörde am Samstag von 18 bis 1 Uhr ihre Pforten, um über 2.300 Interessierte in der Dienststelle willkommen zu heißen und die Möglichkeit zu bieten, die beeindruckende Lichtkunst „Data to Light“ von Florian Mehnert zu begehen. Der Künstler war erneut selbst anwesend, um in sein Kunstwerk einzuführen. Daneben hatten die Besucher_innen zu den elektronischen Klängen der stadtbekannten DJs Sample Samurai und vom STR.711.KOLLEKTIV DGeorge und Dan Ostendorf die Gelegenheit, durch die Lichtinstallation oder die Sonderausstellung der Künstlerin Christiane Schauder zu schlendern. Dies nutzte etwa auch Stuttgarts Oberbürgermeister Dr. Frank Nopper und stattete uns einen Besuch ab. Für das Interesse danken wir, für fühlen uns als Teil der Kulturlandschaft gut aufgehoben, schließlich gehört es auch zu unserer Arbeit, uns und unsere Arbeit in vielfältiger Weise zu präsentieren und insbesondere auch jungen Menschen für unsere Themen zu sensibilisieren.

So waren Themen des Datenschutzes und der Informationsfreiheit derart aufbereitet, die Besucher_in-

nen auf ganz unterschiedliche Weise anzusprechen und für diese verhältnismäßig jungen Bürgerrechte zu interessieren. So klärten in kurzen Texten in Bilderrahmen, Plakaten und Bodenklebern präsentierte Fragen wie „Wusstest Du schon, dass es für Schneewittchen anders gelaufen wäre, wenn im Land hinter den sieben Bergen auch die DS-GVO gelten würde?“ oder „Wusstest Du schon, dass Deine Eltern Deinen Insta-Account erben?“ und kuriose Datenschutzfälle mit einem Augenzwinkern über Datenschutz auf, über QR-Code lieferten wir online weiterführende Informationen zu den einzelnen Themen, unser Pressestand war rege besucht.

Auch das LIFG-Quiz der Abteilung Informationsfreiheit und weitere spielerische Angebote gemeinsam mit der Landeszentrale für politische Bildung – eine schöne Zusammenarbeit – fanden erneut großen Zuspruch. Viele Gäste kamen hierdurch zum ersten Mal mit der Informationsfreiheit in Berührung.

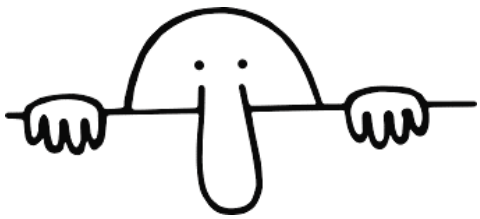
Das Thema „Bürgerrechte“ wurde darüber hinaus mittels einer exklusiven Ausstellung zu Leistungssportler_innen aus der Geschichte des olympischen Sports für die LNM-Gäste aufbereitet – Sportler_innen, die staatlich vereinnahmt wurden und ihre Freiheitsrechte nicht selbstbestimmt nutzen konnten.

Ein besonderes Highlight des Abends stellte auch die Lese-Performance „Art of Being … Oberserved“ der Autoren Jürgen Reuß und Stephan Kuß dar. Gemeinsam mit der Schauspielerin Laura-Sophie Warachewicz präsentierten die Autoren in der 12. Folge der Freiburger Erfolgsreihe „Art of Being“ ein extra für uns kreiertes panoptisches Observatorium in Stuttgart.

Nicht zuletzt der zufällig im Treppenhaus aufgeschnappte Kommentar einer Besucherin zu ihrer Begleitung „Was ist das denn für eine coole Behörde?! Hier möchte ich auch arbeiten“ ist für uns Grund genug, auch im Jahr 2024 wieder Teil der Langen Nacht der Museen zu sein, um Bürger_innen auf diese unkonventionelle Weise zu erreichen und für den Datenschutz und die Informationsfreiheit zu begeistern. Sollte die Besucherin diesen Text hier lesen – nur zur Info: DJs sind üblicherweise nicht bei uns. Aber unsere Themen sind wirklich gut und wichtig, die Arbeit bei uns im Team ist sinnstiftend!

Bilder: LfDI BW

Sabine Keitel von der Landeszentrale für politische Bildung und Sabine Grullini vom LfDI, Data-to-Light-Künstler Florian Mehnert sowie Jürgen Reuß, Laura-Sophie Warachewicz und Stephan Kuß bei ihrer Leseperformance.



ART OF BEING … OBSERVED

Im Auftrag des Datenschutzes: Laura-Sophie Warachewicz, Jürgen Reuß, Stephan Kuß

👉 Samstag, 25.3. / 19:30 / 21 Uhr / LfDI BW / Lautenschlagerstr. 20 / 70173 Stuttgart (Mitte)

In der 12. Folge ihrer Erfolgsreihe Art of Being spannen die Freiburger Autoren Jürgen Reuß und Stephan Kuß ein panoptisches Observatorium für den LfDI Baden-Württemberg auf. Art of Being … Observed ist eine Leseperformance quer durch die Literatur: Nichts haben sie selbst geschrieben, alles wurde abgelauscht. Präsentiert wird die literarische Glotz-, Guck- und Horch-Revue von der Schauspielerin Laura-Sophie Warachewicz und den beiden Kompilatoren der Reihe in der Lichtkunst von Florian Mehnert im Rahmen der Langen Nacht der Museen in Stuttgart.

Zeichnung: Wikimedia Commons

Handzettel zur Leseperformance Art of Being … Observed.

Datenschutz als Kulturaufgabe

Kulturarbeit vernetzt

Zum Programm der Langen Nacht der Museen 2023 – eine wunderbare Veranstaltung, um unsere Dienststelle für die Stadtgesellschaft zu öffnen – hat der Kulturbereich mit der Leseperformance „Art of Being … Observed" beigetragen. Die eigens für uns erstellte Textcollage zu Überwachungsphantasien quer durch die Literaturgeschichte wollen wir auch 2024 präsentieren – in Stuttgart oder an einem anderen Ort im Ländle.

Die Vernetzung mit Hochschulen und weiteren Kooperationspartnern haben wir vorangetrieben. So etwa mit dem Internationalen Zentrum für Kultur- und Technikforschung (IZKT), hier haben wir etwa eine Veranstaltungsreihe unterstützt und über die Regulierung von KI diskutiert. Mit der Stadtbibliothek wollen wir unsere Zusammenarbeit stärken. Nicht nur sind wir sehr gerne vor Ort mit unseren Referent_innen, wir fassen künftig partnerschaftlich generationenübergreifende Projekte zu Digitalisierungsthemen ins Auge.

Maßgebliche Entwicklungen im Blick

Digitalisierung – das heißt immer: Datenverarbeitungen diskursiv zu begleiten. Das hat der Gesetzgeber den Aufsichtsbehörden im Artikel 57 der DS-GVO zur Aufgabe gemacht. Wir sollen

» *maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken.* «

Wir nutzen Methoden und Sichtweisen aus der Kunst und der kulturellen Bildung, um an Kulturtechniken des Digitalen zu arbeiten und um die Öffentlichkeit aufzuklären und zu sensibilisieren (vgl. hierzu den Beitrag Datenschutz als Kulturaufgabe im Tätigkeitsbericht 2022, S. 69ff.). Wir setzen uns auch in einem abstrakteren und allgemeineren Sinn mit gesellschaftlichen Fragestellungen auseinander, die durch die Digitalisierung und Verbreitung intelligenter künstlicher Systeme die gegenwärtigen und zukünftigen Lebenswirklichkeiten bestimmen. Wir wollen dabei an einem diskursiven Raum mitarbeiten, in welchem über Digitalisierung und Künstliche Intelligenz über Fachgrenzen hinweg nachgedacht und verhandelt werden kann – Stichwort ist hier Interdisziplinarität, um gesamtgesellschaftliche Herausforderungen zu fassen –, und haben bei unserer jährlichen KI-Woche Menschen zu Gast, die einen frischen, fremden und nachdenklichen Blick auf Künstliche Intelligenz werfen.

☛ Was Kathrin Passig zu KI sagt

Kathrin Passig hat bereits bei unserer KI-Woche 2022 in ihrem Eröffnungsvortrag „Die Vergangenheit der Zukunft: 70 Jahre Künstliche Intelligenz" eindrücklich beschrieben, dass der Begriff der KI inflationär genutzt wird, beinahe als Synonym für das, was gerade aktueller Stand der Technik ist, was gerade schon oder gerade noch nicht machbar ist, „alles was neu ist und teuer". Der Verzicht auf den Begriff läge näher als ihn zu nutzen. Vor allem empfahl Passig, „genau zu sagen, was passiert", „Firmen und Verfahren konkret", und „wenn etwas undurchschaubar ist: die Gründe dafür präzise benennen", sowie nicht „so zu formulieren, als machte eine Maschine etwas von ganz alleine." Sie empfahl „un-magische Wörter zu finden" und selbst „bei abstrakten Überlegungen konkrete Technik" zu benennen.

Kathrin Passig: Die Vergangenheit der Zukunft: 70 Jahre Künstliche Intelligenz:
tube.bawü.social/w/4uvgRtUxuDAPRHUpQTUEqL

Der Bereich Datenschutz als Kulturaufgabe hat sich – gemeinsam mit unserem KI-Koordinator in diesem Jahr federführend – bei Koordination, Programmierung und Umsetzung dieser Veranstaltungsreihe unter dem Titel „Menschendaten. Die Maschine spricht – wer verantwortet KI?" einge-

bracht. (Einen ausführlichen Bericht finden Sie im Kapitel KI-Woche beim LfDI, S. 34ff.)

Mehr Infos:

KI-Woche 2023 des LfDI: www.baden-wuerttemberg.datenschutz.de/ki-woche-2023

Gezähmte Bots: Wer soll KI regulieren – und wie?: www.izkt.uni-stuttgart.de/veranstaltungen/Gezaehmte-Bots-Wer-soll-KI-regulieren--und-wie-00002

Mit Künstlicher Intelligenz gesellschaftlich umgehen

Feedbackschleifen

Früher hieß es Kybernetik, jetzt Künstliche Intelligenz. Alles neu? Technisch gesehen wahrscheinlich nicht. Aber neu ist, in welchem Maße eine technische Entwicklung, die durch immense Speicherkapazitäten und enormer Datenmengen profitiert, weltweit und im Alltag nutzbar geworden ist. Fast unter der Hand sind Datenanalyse und Vorhersage zum bestimmenden Instrument im „Data Wonderland" geworden.

Für den Philosophen und Mathematiker Rainer Mühlhoff (Die Macht der Daten, 2023) ist Künstliche Intelligenz dabei keine bloße Technik, die in Maschinen (z. B. selbstfahrenden Autos) oder Robotern verbaut ist, und die uns dann als Artefakt gegenübersteht, KI ist vielmehr eine soziale Technologie, die den Menschen quasi einbaut, eine Querschnittstechnologie, die Menschen, Maschinen Kultur, Technik, Ökonomie, materielle und ideelle (= symbolische) Aspekte umfasst. Künstliche Intelligenz, gedacht als ein Mensch-Maschine-Netzwerk, beruht, und hier wird es für den Datenschutz interessant, ganz eminent auf der Ordnung von Daten, und zwar von unseren Daten.

Doch wo werden diese Daten erhoben, wo kommen sie her? Die Antwort darauf lautet: von überall her. Legal oder illegal, aus Europa und aller Welt, mit Zustimmung von Betroffenen oder ohne, urheberrechtlich geschützt oder frei, sind es vor allem Nutzer_innen-Daten verschiedenster Anwendungen und Datensammlungen im Netz. Generative Modelle, die im Moment für den KI-Boom stehen, wurden und werden mit menschlichem Wissen, mit allem aus dem Netz, was nicht niet- und nagelfest ist, gefüttert und trainiert. Sie werden von den Milliarden Nutzer_innen durch Feedbackschleifen nachjustiert – jeder Prompt, jeder Kommunikationsschritt mit ChatGPT und Co. macht das Ding prinzipiell „schlauer" und speist Nutzungsverhalten der Anwender_innen mit ein.

Über die Macht der Daten

Rainer Mühlhoff: Die Macht der Daten. Warum künstliche Intelligenz eine Frage der Ethik ist, Osnabrück 2023: rainermuehlhoff.de/media/publications/m%C3%BChlhoff_2023_die_macht_der_daten.pdf

Gemeinsamer Forschungsbeitrag von Rainer Mühlhoff und Hannah Ruschemeier: rainermuehlhoff.de/media/publications/telemedicus-2022-tagungsband-isbn-978-3-8005-1857-9.pdf, S. 38–67

Paola Lopez: Bias: Ein Begriff voller Ambiguität: tube.bawü.social/w/kjvbpYfYBLdbMSb23qS7xX

Paola Lopez, Artificial Intelligence und die normative Kraft des Faktischen, Heft 863, April 2021: www.merkur-zeitschrift.de/artikel/artificial-intelligence-und-die-normative-kraft-des-faktischen-a-mr-75-4-42

Die Ordnung der Daten

Wie funktioniert das genau? Grundlage ist neben der enormen Rechenleistung der Computer das Prinzip der Mustererkennung in Daten. Je mehr – und wir reden von gigantischen Datenmengen, die in den letzten beiden Jahrzehnten akkumuliert wurden – (und je „qualitätsvoller" die) Daten, um so aussagefähiger und präziser die Mustererkennung und Zuordnung. „Wahrscheinlich", das heißt regelkonform, gehört ein Datum zu dieser oder jener Kategorie, wahrscheinlich wird in Zukunft dann Folgendes der Fall sein. Mustererkennung und Wahrscheinlichkeitsrechnung sind zwei Seiten derselben Medaille: Daten werden kategorisiert. Wenn in der Vergangenheit oft A auf B folgte, wird

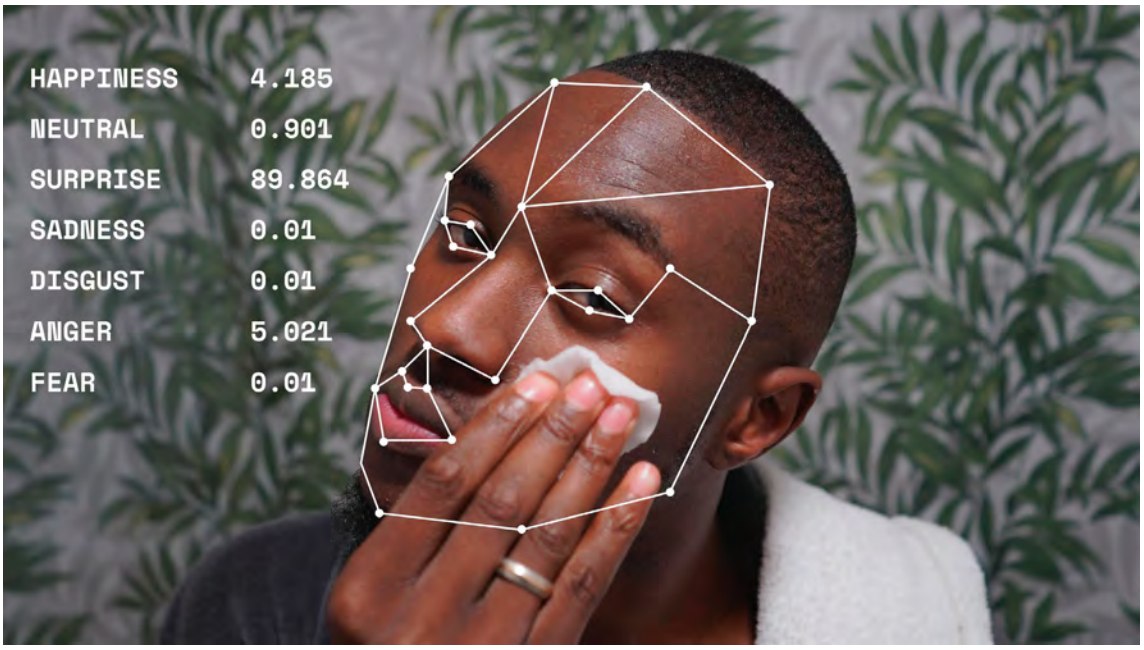


Bild: Image by Comuzi / © BBC / Better Images of AI / Mirror D / CC-BY 4.0

Wem steht welches Gefühl (und wie viel davon) ins Gesicht geschrieben?

das wahrscheinlich auch für die Zukunft gelten. Wenn A meistens mit C auftritt, kann mit einiger Wahrscheinlichkeit von A auf C geschlossen werden. Aus der Erkennung von Mustern wird das, was in der Fachliteratur „predictive analytics" heißt, für die Zukunft abgeleitet.

Für die Werbeindustrie hat das einigen Reiz: Wenn soundso viele Kunden Produkt A und C interessant finden, wird wahrscheinlich auch Kunde X, der A interessant findet, für C empfänglich sein. Empfehlungsmarketing mag der eine positiv bewerten, der andere als störend empfinden.

Anders sieht es aber mit Praktiken im öffentlichen Sektor aus, in denen staatliche Reaktionen bzw. Sanktionen genau nicht auf das allgemein Wahrscheinliche, sondern auf den konkreten (womöglich unwahrscheinlichen) Fall passen müssen. In Österreich ist der Einsatz von „predictive analytics" durch Job-Center immerhin hochumstritten. Jemanden beispielsweise von Fördermaßnahmen für den Arbeitsmarkt auszuschließen, weil es „wahrscheinlich nichts bringt": Das verstößt gegen dessen Menschenwürde, da er oder sie zum „Objekt" von Berechnungen gemacht wird. Es wird die Freiheit genommen, es in Zukunft anders zu machen als es die eigene Vergangenheit (oder auch nur: die Praxis der Vergleichsgruppe) nahelegt.

„Menschendaten", so haben wir unsere diesjährige KI-Woche überschrieben. Es geht um unsere Daten – und um die transparente oder weniger transparente Verarbeitung dieser Daten. Natürlich geht es auch um Macht. Das ergibt sich aus der schieren Menge an Daten, die ein Unternehmen haben muss, um überhaupt mitspielen zu können bei Entwicklung, aber auch Anwendung von KI. Es geht um Abhängigkeiten von Ressourcen und Applikationen und um mögliche, auch öffentliche, Alternativen zu den großen Akteuren. Kann es aber bereits die Anonymisierung von personenbezogenen Daten in punkto informationelle Selbstbestimmung richten (und blieben dann lediglich Urheberrechtsfragen stehen? Hat auch ein Sprachstil Personenbezug)? Müssen Daten „richtig" sein? Was ist mit all den „halbwahren" Biographien, zu denen man Chatbots so publikumswirksam befragen kann?

Was ist überhaupt vom Halluzinieren von Sprachmodellen zu halten, die ja, so ist verschiedentlich zu vernehmen, die gängigen Suchmaschinen bald ersetzen könnten?

☛ **Léon Botton und Bernhard Schölkopf feiern Sprachbots, irgendwie:**

„Die Erfindung einer Maschine, die nicht nur Geschichten, sondern auch alle ihre Variationen schreiben kann, ist […] ein Meilenstein in der Geschichte der Menschheit. Sie ist mit der Erfindung des Buchdrucks verglichen worden. Ein passenderer Vergleich wäre vielleicht,was die Menschheit lange vor dem Buchdruck, der Schrift oder gar den Höhlenmalereien geprägt hat: die Kunst des Geschichtenerzählens."

www.faz.net/aktuell/wirtschaft/kuenstliche-intelligenz/ki-und-sprache-wie-chatgpt-und-co-uns-neue-zugaenge-ermoeglichen-koennen-19391133.html

Die Datenerhebung als eminente Grundlage von datenbasierter KI rechtlich abzusichern und für die Zukunft zu regeln, ist eine Riesenaufgabe für den Gesetzgeber und schließlich für die die Einhaltung des Rechts zuständigen Aufsichtsbehörden. In Europa soll die KI-Verordnung das leisten (und nicht nur Europa will regulieren oder hat bereits reguliert). Die DS-GVO hat bei personenbezogenen Daten einiges beizusteuern.

Jugend- und Medienbildung

Bereits ein Jahr nach dem erfolgreichen Relaunch der Internetplattform YoungData durch die Datenschutzkonferenz der Länder und des Bundes hat das behördenübergreifende Projekt den dritten Platz beim Tommi-Award in der Kategorie „Jugendpreis Bildung" gewonnen. O-Ton der Jugendjury: „Vor allem haben wir verstanden, dass es beim Thema Datenschutz um uns als Menschen geht und nicht um Daten." Die Plattform bereitet Datenschutzthemen und Themen der Informati-

Bild: Jamillah Knowles / Better Images of AI / Data People / CC-BY 4.0

So wie Menschen im Analogen beim Spazierengehen Schatten werfen, können im datengetriebenen Zeitalter auch digitale Schatten von ihnen entstehen.

onsfreiheit nah an deren Lebenswirklichkeit für eine junge Zielgruppe auf, wir unterstützen diese Plattform und beteiligen uns im Redaktionsteam.

Videoclips für Kinder und Jugendliche

Im Dezember machten sich einige Kolleg_innen aus Datenschutz und Informationsfreiheit auf den Weg nach Frankfurt, um gemeinsam mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. und der Medienagentur „Zeitgenossen" neue Videos für die Reihe „Datenschutz – leicht erklärt" aufzuzeichnen. Wir haben drei neue Datenschutz-Videos gedreht – die Reihe nun ergänzt um einen allgemein einordnenden Clip „Datenschutz – Warum?", um einen Clip zu „Tracking" mit unserem Kollegen Dr. Walter Kicherer sowie zu „Gaming" mit unserer Kollegin Tamara Damjanovic. Neu hinzugekommen und erweitert wurde die Reihe durch drei Videos „Informationsfreiheit – leicht erklärt", welche unsere Kolleginnen von der Abteilung Informationsfreiheit für zwei Schülerinnen intensiv gestaltet haben.

☛ YoungData

Das Jugendportal zum Thema Datenschutz und Informationsfreiheit YoungData: youngdata.de

Jurybegründungen zur Verleihung des Kindersoftwarepreises Tommi für YoungData:

tommi.kids/kindersoftwarepreis/gewinner/gewinner-2023

☛ Datenschutz – leicht erklärt

Die neuen und vorherigen Videos, die im Schulunterricht im Rahmen von „Datenschutz geht zur Schule" bereits seit 2022 erfolgreich von Lehrer_innen und ehrenamtlich tätigen Dozent_innen eingesetzt werden, stehen hier:

www.baden-wuerttemberg.datenschutz.de/datenschutz-leicht-erklaert

www.datenschutz-leicht-erklaert.de

Bilder: LfDI BW

Tobias Keber vor der Kamera bei der Aufzeichnung der Clips zu "Datenschutz – leicht erklärt" – und hinter der Kamera dabei, Tetris durchzuspielen.

Neues aus der Bußgeldstelle

Im Zeitraum vom 1. Januar 2023 bis zum 31. Dezember 2023 hatten wir insgesamt 185 Neueingänge in der Bußgeldstelle zu verzeichnen. Die Zahl der neu anhängigen Verfahren blieb damit im Vergleich zum Vorjahr auf einem konstant hohen Niveau. Insgesamt wurden 211 Verfahren abgeschlossen, womit die Erledigungszahl im Vergleich zum Vorjahr um fast 25 Prozent gestiegen ist. Viele kleinere Fälle konnten wir abschließen, die bei uns in der Bußgeldstelle aufliefen, bei denen ein Bußgeld nicht in Betracht kam, da sich entweder Hinweise auf gravierendes Fehlverhalten nicht erhärteten oder wir feststellen konnten, dass die Verantwortlichen einsichtig waren und glaubhaft darlegen konnten, dass sie aus ihren datenschutzrechtlichen Verfehlungen gelernt haben. Es wurden insgesamt 11 Bußgeldbescheide erlassen, die sich gegen natürliche Personen richteten und die rechtskräftig sind. Die Gesamtsumme der festgesetzten Geldbußen lag im Berichtszeitraum bei 15.800 Euro.

Dass wir ausschließlich Bußgelder gegenüber natürlichen Personen erhoben, lag unter anderem auch daran, dass die offene Rechtsfrage, ob sich DS-GVO-Bußgeldverfahren unmittelbar gegen Unternehmen richten könne noch auf europäischer Ebene zur Entscheidung anstand (EuGH, Urteil vom 5. Dezember 2023, Az. C-807/21). Wir haben zu dieser EuGH Entscheidung ausführlich in der 34. Folge unseres Podcasts „Datenfreiheit“ gesprochen und sie eingeordnet. Gestärkt durch diese Rechtsprechung werden wir im kommenden Jahr einige Verfahren gegen Unternehmen beenden können.

Bußgeldverfahren im Bereiche des Datenschutzrechts sind stets mit einem erheblichen Ermittlungsaufwand verbunden. Im Ordnungswidrigkeitenrecht gilt analog zum strafrechtlichen Verfahren der Amtsermittlungsgrundsatz. Bei datenschutzrechtlichen Verstößen handelt es sich noch immer um ein großes Dunkelfeld, welches erst durch umfangreiche Kontrollen und Ermittlungen in seinem Ausmaß ersichtlich wird.

☛ EuGH, Urteil vom 5. Dezember 2023, Az. C-807/21:

curia.europa.eu/juris/document/document.jsf?text=&docid=280325&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=5089467

„Tracking“ in Partnerbeziehungen

Der Gedanke an staatliche Überwachung auf Schritt und Tritt dürfte für Unbehagen und Entrüstung sorgen, insbesondere wenn diese verdeckt geschieht und zur heimlichen Ansammlung von Informationen dient. Zum Schutz der Bürger_innen vor derartigen staatlichen Eingriffen existieren in unserem demokratischen Rechtssystem hohe gesetzliche Anforderungen, die erfüllt sein müssen, damit eine solche Überwachung rechtmäßig erfolgen kann. Sie stehen in der Regel im Kontext von Schwerstkriminalität und extremen Sicherheitsbedrohungen. Heimliche Überwachungsmaßnahmen sind zudem zeitlich begrenzt und unterliegen dem Richtervorbehalt. Nach dem Grundsatz der Verhältnismäßigkeit muss zudem stets begründet werden, warum weniger einschneidende Maßnahmen nicht ausreichen. Nach Beendigung der Überwachung ist die Benachrichtigung der Betroffenen vorgeschrieben.

Zunehmend greifen auch Privatpersonen, die häufig in einem besonderen sozialen Näheverhältnis zueinanderstehen, auf solche Mittel zurück. Dies passiert in vielen Fällen ohne Einwilligung oder Wissen der überwachten Person. Misstrauen oder sogar krankhafte Eifersucht im zwischenmenschlichen Zusammenleben stellt oft die Motivationslage der überwachenden Person dar. Wir stufen den Einsatz von Trackingsystemen durch Privatpersonen zur Ausspionage des Aufenthaltsortes anderer Personen als schwerwiegenden Eingriff in die Privatsphäre ein und ahnden diesen konsequent mit Bußgeldern. Allerdings ist dabei der Ermittlungsaufwand stets groß. So werden von uns Informationen benötigt, welche Mobilfunknummer mit dem

gefundenen Bewegungstracker verbunden ist, insbesondere der Namen des Anschlussinhabers. Hierbei leistet uns die Polizei häufig wertvolle Hilfe.

In einem jüngsten Fall haben wir ein hohes Bußgeld gegen eine Frau verhängt, die über einen längeren Zeitraum einen sogenannten Bewegungstracker an einem fremden Kraftfahrzeug angebracht hatte. Diese lediglich münzgroßen Geräte zeigen den genauen Standort eines Gegenstandes in Echtzeit an. Doch es ging der Frau nicht um den Standort ihres Mannes, sondern um den der vermuteten Geliebten beziehungsweise den Standort von deren Fahrzeug. Ziel war es, Beweise für eine außereheliche Beziehung zu sammeln und den Ehepartner damit zu konfrontieren. Die Geschädigte erstattete, nachdem das Gerät gefunden wurde, folglich Anzeige bei der Polizei. Die eindeutige Rechtslage, die getätigten Ermittlungen und die Beweislage sorgten in diesem Fall für Klarheit und führten zur Verhängung eines Bußgeldes.

Immer wieder führen wir aber auch Verfahren im Zusammenhang mit Tracking, die sich insbesondere auf bereits getrenntlebende Ehepaare und Sorgerechtsstreitigkeiten beziehen. Insbesondere fühlen sich die Ehemänner als Fahrzeughalter noch dazu berechtigt, dieses mit einem Bewegungstracker auszustatten. Dabei übersehen sie, dass die möglicherweise umstrittenen Eigentumsverhältnisse für die datenschutzrechtlichen Belange unbeachtlich sind.

Wenn die Kundendatei im Müllsack landet: Pizzalieferanten als Großdatenverarbeiter

In einem aktuellen Fall wurde dem Betreiber eines Pizzalieferservice vorgeworfen, dass dieser seit mehreren Jahren die ausgedruckten Kassenbelege nach Auftragserledigung und Auslieferung der Speisen innerhalb seiner Verkaufs- und Lagerräume vor der finalen Entsorgung offen in Abfall-Behältnissen oder Müllsäcken ansammelt und zwischenlagert.

Dem verantwortlichen Gastronomiebetrieb dürfte jedoch die Bedeutung und Werthaltigkeit seiner über Jahre angesammelten Kundendatenbank, die er in Müllsäcken „lagerte“, gar nicht bewusst gewesen sein. Entdeckt wurde der Verstoß durch den Ordnungsdienst einer Großstadt. Diese entdeckten zwei große Müllsäcke neben einem Altglascontainer. In diesen befanden sich Kassenbelege eines lokalen Pizzalieferdienstes mit den vollständigen Kundendaten, wie Vor- und Nachname, Adresse, Handynummer, Bezahlart, bestellte Speisen und Beträge.

Aus hygienischen Gründen wurde auf eine händische Einzelzählung weitgehend verzichtet. Die Kassenbelege stammten überwiegend noch aus der pandemischen Zeit. Um eine nahezu genaue Anzahl zu bestimmen, wurde bei der Stadt unter besonderen Sicherheitsvorkehrungen 1.000 einzelne Belege abgezählt und das genaue Gewicht des Stapels mit einer Briefwaage ermittelt. Infolge des somit ermittelten Gewichts erfolgte eine Hochrechnung, so dass man auf 7.745 Belege kam. Zugunsten des Gewerbetreibenden wurde hier mit hohen Abzügen gearbeitet. Dieser machte seinen unzuverlässigen Mitarbeiter für die unsachgemäße Müllentsorgung verantwortlich, übersah aber hierbei, dass er gemäß Art. 4 Nr. 7 DS-GVO verantwortlich ist. Auf Grund der Gesamtumstände hatten wir den begründeten Verdacht, dass es sich bei den gefundenen Kassenbelegen nur um „die Spitze des Eisberges“ handelte.

Daher erwirkten wir beim Amtsgericht einen Durchsuchungsbeschluss für die Betriebsräume. Die Polizei durchsuchte für uns die Geschäftsräume und konnte auch ausreichend Beweismittel auffinden. Unser Verdacht einer systematischen rechtswidrigen Datenverarbeitung bestätigte sich aufgrund der Vielzahl an gelagerten Müllsäcken mit Kassenbelegen.

Gemäß Art. 5 Abs.1 lit. f DS-GVO müssen verantwortliche Stellen personenbezogene Daten so verarbeiten, dass die angemessene Sicherheit der Daten gewährleistet ist. Dies umfasst den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtig-

ter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen. Dies schließt ein, dass Unbefugte keinen Zugang zu den Daten haben dürfen.

Die jahrelange unsachgemäße Ansammlung und Lagerung der Kassenbelege in den Gewerberäumen und die rechtswidrige Entsorgung führte dazu, dass die personenbezogenen Kundendaten für jeden zugänglich waren, insbesondere für andere Bedienstete oder auch Kunden.

Dies galt erst recht für die finale Entsorgung des Datenmülls. Die praktizierte Verfahrensweise entsprach keinesfalls einer technisch ordnungsgemäßen Datenentsorgung. Hier wurden weder geeignete Gerätschaften zur datenschutzkonformen Datenlagerung und -vernichtung eingesetzt noch ein zertifizierter Entsorgungsbetrieb für eine fachgerechte Zwischenlagerung und Entsorgung des Datenmülls beauftragt.

Wir gehen davon aus, dass das festgesetzte Bußgeld im mittleren vierstelligen Bereich dazu führt, die betriebsinternen Prozesse anzupassen.

Vorsicht beim Einsatz einer Dashcam

Die Fallbearbeitungszahlen in Sachen rechtswidriger Aufzeichnungen im Straßenverkehr mit sogenannte Dashcams sind seit Jahren sehr hoch. In den überwiegenden Fällen werden handelsübliche Kameras im unteren Preissegment durch Privatpersonen verwendet, die eine datenschutzkonforme Einstellung entweder gar nicht oder nur mit etwas größerem Aufwand ermöglicht.

Platziert werden Dashcams im Bereich der vorderen Windschutzscheibe. Je nach Ausstattung können diese nach vorne und hinten das Verkehrsgeschehen beobachten und aufzeichnen. Dabei wird auf diese Art und Weise ein erhebliches Datenvolumen erzeugt. In vielen Fällen ist die Kamera manuell so eingestellt, dass diese mit Beginn der Stromversorgung des Pkw startete und während des Betriebs automatisch – ohne dass die Kamera manuell ein- und ausgeschaltet werden muss – die gesamte Fahrt aufzeichnet.

Dabei ist die Rechtslage eindeutig, dass ein derartiges Anfertigen von Bildaufzeichnungen als besondere Form der Datenverarbeitung rechtwidrig und unzulässig ist. Von einer Dashcam wird nicht nur das Kennzeichen des vorausfahrenden Fahrzeuges abgebildet, sondern insbesondere auch der gesamte Straßenverkehr erfasst.

☛ Orientierungshilfe Videoüberwachung

Die Datenschutzkonferenz hat im Jahr 2020 die Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen herausgegeben, in der auch Dashcams angesprochen werden. Mehr dazu:

www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf, S. 32ff

Soweit Dashcams in öffentlich zugänglichen Bereichen filmen, ist deren Einsatz an Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zu messen. In den überwiegenden Fällen ist die videographische Überwachung des öffentlichen Straßenraumes zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke nicht erforderlich. Dabei überwiegen gerade die schutzwürdigen Interessen der von der Videoaufzeichnung erfassten Verkehrsteilnehmer.

Die (versteckte) Beobachtung und Aufzeichnung von Straßenverkehrsteilnehmenden in zumindest nicht geringem Umfang stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen und damit einen schwerwiegenden Datenschutzverstoß dar (VG Göttingen, Beschluss vom 12. Oktober 2016, Az. 1 B 171/16, Rz. 51; VG Ansbach, Urteil vom 12. August 2014, Az. 4 K 13.01634, Leitsatz Nr. 3; OLG Celle, Beschluss vom 4. Oktober 2017 – 3 Ss (OWi) 163/17, Leitsatz; OLG Stuttgart Beschluss vom 4. Mai 2016, 4 Ss 543/15 – zitiert nach juris). 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 (BGH,

Urteil vom 15. Mai 2018, Az. VI ZR 233/17, Rz. 19, 26 – zitiert nach juris).

Auch sind diese Aufzeichnungen nicht von einer Einwilligung der betroffenen Personen gemäß Art. 6 Abs. 1 Satz 1 lit. a DS-GVO umfasst.

Ein zulässiger Einsatz der Dashcam ist ausschließlich dann gegeben, wenn erst im Falle eines Unfalls oder einer Gefahrenbremsung die Aufnahme mittels eines durch Unfallsensoren ausgelösten automatisierten Überschreibungsschutzes gespeichert werden. Ausschließlich für die Dokumentation und zur Beweiserhebung von erheblichen Verfehlungen im Straßenverkehr bei der eine unmittelbare Betroffenheit vorliegt, wäre auch das manuelle Starten im Pre-Recording zulässig. Die gespeicherten Aufnahmen sind unmittelbar zu löschen, wenn diese nicht mehr als Beweismittel benötigt werden. Ein Veröffentlichen der Aufnahme im Internet etwa ist unzulässig.

Unsere Behörde befasste sich im Berichtszeitraum mit folgendem Vorgang: Ein ehemaliger Fahrlehrer filmte mit einer Dashcam ein aus seiner Sicht unrechtmäßiges Vorgehen eines vorausfahrenden Fahrers. Er machte auf sich mit seiner Lichthupe aufmerksam, der Vorausfahrende hielt an. Es folgte ein Gespräch zwischen diesen beiden, der ehemalige Fahrlehrer veranschaulichte dem Verkehrssünder dessen Fehlverhalten mit den Dashcam–Aufnahmen, die er gemacht hatte. Der Fahrer, der mit der Kamera aufgezeichnet wurde, verständigte die Polizei. Der Vorfall wurde zur Anzeige gebracht und die Dashcam mit den Aufzeichnungen mit richterlicher Anordnung beschlagnahmt.

Wir haben uns im weiteren Verlauf mit dem Sachverhalt im Rahmen eines Bußgeldverfahrens befasst. Nach Abwägung aller Zumessungskriterien erschien für uns die Festsetzung einer Geldbuße im unteren vierstelligen Bereich als wirksam, hinreichend abschreckend und verhältnismäßig. Dabei wurde auch berücksichtigt, dass die Aufzeichnungen zweckwidrig als Instrument der Verkehrserziehung eingesetzt wurden. Für Privatpersonen besteht kein berechtigtes Interesse an einer beweiserheblichen Aufzeichnung des Fahrverhaltens anderer, um „erzieherisch“ auf diese einzuwirken.

Unrechtmäßiger Datenabruf aus Neugierde

In verschiedenen Bereichen werden Datenbanken und Abfragesysteme zur Verarbeitung von personenbezogenen Daten zu festgelegten, eindeutigen und legitimen Zwecken von Arbeitgebenden bereitgestellt, um Aufgaben dienstlicher Natur zu erfüllen. Doch was passiert, wenn diese Datenbanken zu privaten Zwecke eines Mitarbeitenden des öffentlichen Dienstes genutzt werden?

Zwar sieht § 28 LDSG unter anderem vor, dass gegen öffentliche Stellen keine Geldbußen verhängt werden dürfen. Eine „Immunität“ für Mitarbeitende einer öffentlichen Stelle bedeutet dies jedoch nicht. Vielmehr ist von dem oben genannten Grundsatz eine Ausnahme zu machen, wenn das Verhalten eines oder einer Mitarbeitenden der öffentlichen Stelle nicht zuzurechnen ist, das heißt, ein Mitarbeitendenexzess vorliegt.

Die rein private Nutzung eines dienstlich zur Verfügung gestellten Abfragesystems stellt regelmäßig eine eigenmächtige Verarbeitung zu gesetzesfremden Zwecken dar, welche dem Arbeitgeber bzw. der öffentlichen Stelle nicht zuzurechnen ist. Ferner ist der handelnde Mitarbeitende auch nicht als öffentliche Stelle im Sinne des § 2 Abs. 1 oder Abs. 2 LDSG zu qualifizieren. Für zweckwidrige, rechtsgrundlose Verarbeitungen kann dementsprechend gemäß Art. 83 Abs. 5 Buchst. a. DS-GVO eine Geldbuße verhängt werden.

☛ LfDI Baden-Württemberg verhängt erstes Bußgeld gegen Polizeibeamten

www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-erstes-bussgeld-gegen-polizeibeamten

Im Berichtszeitraum wurden erneut Bußgelder wegen der Nutzung dienstlich zur Verfügung gestellte Datenbanken zu privaten Zwecken verhängt.

So überschritt eine Mitarbeiterin eines Klinikums ihren Zuständigkeitsbereich, welcher die Abrechnungen von erbrachten Leistungen betraf, um mehr über ihre neue Nachbarin zu erfahren. Durch den Abruf in dem dortigen Patientenverwaltungssystem konnten nicht nur die vollständigen Personalien der Nachbarin eingesehen werden, sondern auch sämtliche Klinikaufenthalte und Diagnosen.

Erfreulicherweise hatte das Klinikum wesentlich zur Aufklärung des Sachverhaltes beigetragen und auch selbst arbeitsrechtliche Schritte gegen die Mitarbeiterin eingeleitet. Gegen die Betroffene wurde ein Bußgeld in Höhe von insgesamt 2.000,00 Euro verhängt. Bei der Bemessung fanden die Tatsache, dass es sich um einen Erstverstoß handelte und die Betroffene auch arbeitsrechtliche Maßnahmen erhielt, wie auch der Umstand, dass es sich um Daten der besonderen Kategorie nach Art. 9 DS-GVO handelte, Berücksichtigung.

Auch im Bereich der Polizei sind solche zweckwidrigen und rechtsgrundlosen Abfragen Gegenstand von Bußgeldverfahren. So hatte eine Beschäftigte der Polizei diverse Abfragen in dem Meldeportal MeldIT getätigt. So soll in einem Fall eine Berichterstattung im Radio die Betroffene so bewegt haben, dass sie sich dazu entschied, sich weitere Informationen zu den Akteuren der Berichterstattung selbst zu beschaffen. Gegen die Betroffene wurde ein Bußgeld in Höhe von 1.200,00 Euro als wirksam, abschreckend und verhältnismäßig erachtet.

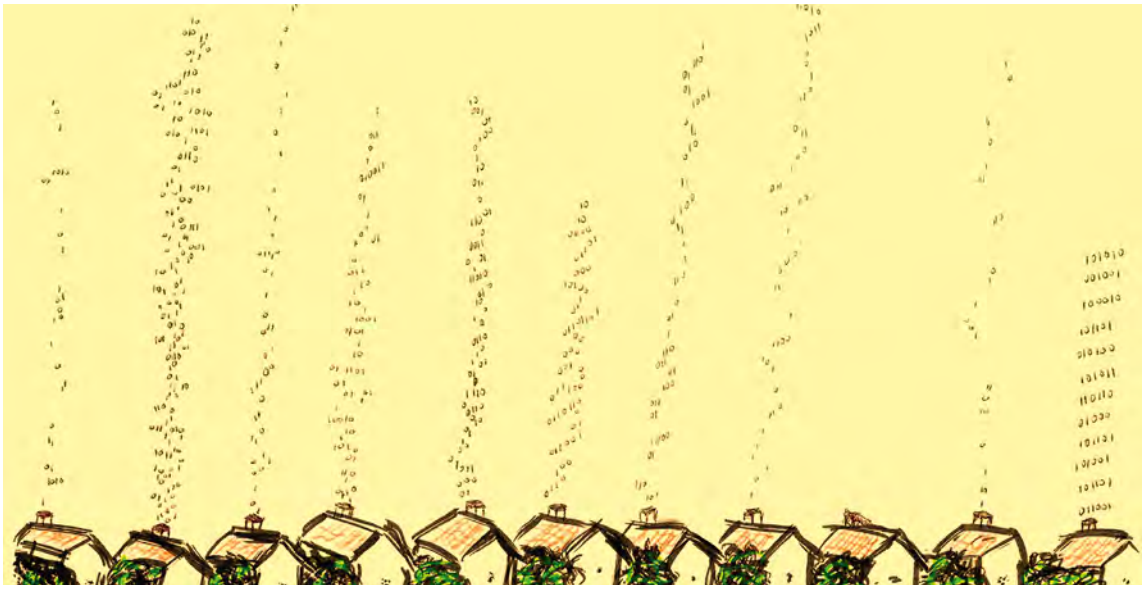


Bild: Joahna Kuiper / Better Images of AI / Little data houses / / CC-BY 4.0

In jedem Haus werden unterschiedliche Daten produziert. Sie gehen nicht jeden etwas an.

Neues aus dem Amt: Innere Sicherheit, Justiz, Kommunalwesen

Keine gute Idee: Private E-Mailadressen für die Arbeit als Gemeinderatsmitglied verwenden

Bereits kurz nach Wirksamwerden der DS-GVO haben wir in unserer Broschüre „Datenschutz bei Gemeinden“ auf die Schwierigkeiten bei der Verwendung von privaten E-Mailadressen durch Mitglieder von Gemeinderäten hingewiesen (. Doch noch immer erreichen uns Hinweise und Beschwerden von Bürger_innen zu diesem Thema. Das Problem: Bei der Tätigkeit als Gemeinderatsmitglied ist die Gemeinde für die Verarbeitungen von personenbezogenen Daten durch die Ratsmitglieder verantwortlich. Doch wie soll die Gemeinde die Rechtmäßigkeit sicherstellen, wenn die Daten bei privaten E-Mailprovidern liegen?

☛ **Broschüre Datenschutz bei Gemeinden**

www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Brosch%C3%BCre-Gemeinden-November-2019.pdf, S. 90 ff, insb. S. 93.

Mitglieder des Gemeinderats sind ehrenamtlich tätig. Im Amt entscheiden sie nach ihrer freien, nur durch das öffentliche Wohl bestimmten Überzeugung. Ähnlich dem freien Mandat von Abgeordneten der Parlamente sind sie also in ihren Entscheidungen frei. Anders als bei den Parlamenten sind Gemeinderäte jedoch kein Organ der Legislative, sondern der Exekutive. Mitglieder des Gemeinderats sind also Teil der Verwaltung. Aus datenschutzrechtlicher Sicht bedeutet dies: Die Gebietskörperschaft Gemeinde ist der für die Einhaltung datenschutzrechtlicher Vorgaben durch die Gemeinderatsmitglieder Verantwortliche. Selbstverständlich ist hierbei die freie Ausübung des Amts zu berücksichtigen. Dies hat jedoch keinen Einfluss auf die grundlegende Pflicht der Gemeinde, ihre Verarbeitungen von personenbezogenen Daten rechtmäßig zu gestalten.

Für ihre Arbeit werden den Gemeinderatsmitgliedern von der Gemeinde regelmäßig Unterlagen zur Verfügung gestellt. Auf Antrag ist der Bürgermeister oder die Bürgermeisterin außerdem verpflichtet, über alle Angelegenheiten der Verwaltung

Bild: blanckstock-stock.adobe.com

Gemeinden sollten Gemeinderäten E-Mailadressen einrichten.

Auskunft zur erteilen. Dabei können den Gemeinderatsmitgliedern auch personenbezogene Daten offenbart werden, beispielsweise wenn sie in Bewerbungsverfahren für Stellen und Ämter einbezogen sind, wenn es um einzelne Bauvorhaben geht oder sonst ein Einzelfall aus der Verwaltung für den Gemeinderat von Interesse ist. Angesichts der Vielzahl an kommunalen Aufgaben sind vielfältige Konstellationen denkbar. Möglich ist darüber hinaus, dass Bürger_innen mit den Mitgliedern des Gemeinderats direkt in Kontakt treten möchten. Dafür stehen oftmals auf den gemeindlichen Websiten Kontaktdaten zur Verfügung.

Die Art und Weise der Informationsvermittlung der Gemeinde an ihre Ratsmitglieder und die Art und Weise der Kontaktaufnahme durch Bürger_innen mit den Ratsmitgliedern muss datenschutzkonform erfolgen. Das bedeutet z. B., dass die Gemeinde die Löschung der Daten sicherstellen muss, wenn diese nicht mehr für die Amtsausübung benötigt werden, etwa wenn das jeweilige Mitglied aus dem Amt ausscheidet. Ganz grundsätzlich muss die Gemeinde für die Integrität und Vertraulichkeit der Daten sorgen, also insbesondere dafür, dass die Informationen keinem Unbefugten gegenüber offenbart werden.

Alles dies ist problematisch, wenn Gemeinderatsmitglieder über ihre private E-Mailadresse von der Gemeinde oder von den Bürger_innen kontaktiert werden. Verwenden Gemeinderatsmitglieder beispielsweise E-Mailadressen aus ihrem beruflichen Kontext, so könnte unter Umständen der Arbeitgeber oder die Arbeitgeberin des jeweiligen Ratsmitglieds darauf zugreifen. Datenschutzrechtlich läge in dieser Konstellation eine Übermittlung der personenbezogenen Daten an den Arbeitsgeber oder die Arbeitgeberin vor, wofür eine Rechtsgrundlage nicht ersichtlich ist. Uns ist auch ein Fall bekannt, in dem die E-Mailadresse der Ehefrau eines Gemeinderatsmitglieds für die Kommunikation mit ihm verwendet wurde. Je nach E-Mailanbieter steht im Übrigen die Frage im Raum, ob dieser die bei ihm gespeicherten Daten angemessen vor dem Zugriff Dritter schützt oder möglicherweise selbst auf die Inhalte im Posteingang des jeweiligen Gemeinderatsmitglieds zugreift, z. B. um passgenaue Werbung anzubieten. Jedenfalls dann, wenn die E-Mails über den reinen Versendungsvorgang hinaus beim E-Mailanbieter gespeichert bleiben, müsste die Gemeinde außerdem als Verantwortliche den Provider als einen Auftragsverarbeiter einbinden, also eine Auftragsverarbeitungsvereinbarung mit dem Anbieter abschließen.

Verantwortliche können die Rechtmäßigkeit ihrer Verarbeitungen sowohl durch organisatorische als auch durch technische Maßnahmen sicherstellen. Das Erreichen eines hinreichenden Schutzes wird jedoch bei der Nutzung privater E-Mailanbieter kaum umsetzbar ein. So wäre es zwar z. B. denkbar, dass Gemeinderatsmitglieder beim Ausscheiden aus dem Amt aufgefordert werden und eine Erklärung unterzeichnen, dass sie sämtliche personenbezogenen Daten aus den Zeiten der Amtsausübung gelöscht haben. Allerdings muss auch das Verhältnis zum E-Mailprovider bedacht werden: Wer prüft beispielsweise dessen Schutzmaßnahmen vor unbefugten Zugriffen auf das E-Mailkonto und stellt sicher, dass eine Löschung endgültig erfolgt? Man kann von Gemeinderäten nicht erwarten, dass sie dies bewerten können. Dies zu tun wäre Aufgabe der Gemeinde. Auch das Schließen einer Vielzahl an Auftragsverarbeitungsvereinbarungen zwischen Gemeinde und E-Mailprovider wird kaum praxistauglich umsetzbar sein. Die Nutzung privater E-Mailadressen bedeutet also ziemlich viel Arbeit für alle Beteiligten, vor allem unnötige Arbeit.

Eine alternative Möglichkeit wäre beispielsweise das Einrichten gemeindlicher E-Mailadressen für die Gemeinderatsmitglieder oder ein Onlineportal, auf dem Gemeinderatsmitglieder (unter Verwendung eines hinreichenden Authentifizierungsverfahrens) die für Ihre Tätigkeit erforderlichen Daten abrufen können. Das Portal oder die Speicherung der gemeindlichen E-Mails würden von der Gemeinde verwaltet. So könnte die Gemeinde ihren datenschutzrechtlichen Pflichten nachkommen.

Im Übrigen bestehen neben den datenschutzrechtlichen Pflichten für ehrenamtlich tätige Gemeinderatsmitglieder ganz grundsätzlich die allgemeinen Verschwiegenheitspflichten. Die Einhaltung derer

für die Gemeinderatsmitglieder zu erleichtern, sollte im Interesse der Gemeinden sein.

Die Verwendung privater E-Mailadressen mag gerade bei ehrenamtlich tätigen Gemeinderatsmitgliedern für eine Gemeinde praktisch sein, aus datenschutzrechtlicher Sicht ist dies jedoch nicht zu empfehlen. Dies birgt eine Vielzahl an Risiken, weswegen wir dringend davon abraten. Bessere Lösungen sind gemeindliche E-Mailadressen oder ein kommunales Onlineportal, in dem die Mitglieder relevante Unterlagen abrufen können. Wir stehen den verantwortlichen Gemeinden gerne mit unserem Rat zur Seite und unterstützen, dass der Arbeitsaufwand reduziert wird für alle Beteiligten und zugleich datenschutzrechtlich tragfähige Lösungen vorgehalten werden. Auch sind wir etwa mit den Vertretungen der Gemeinden, Stadt- und Landkreisen im Austausch. Mit Blick auf die Vielzahl kommunaler Aufgaben können Prozessveränderungen gerade für kleine Gemeinden eine größere Herausforderung darstellen. In Zusammenarbeit mit dem Gemeindetag werden wir deswegen weitere Unterstützungsmöglichkeiten eruieren, beispielsweise wie wir unser Informationsangebot zu dem Thema ausbauen könnten. Einheitliche, klare Vorgaben reduzieren für alle Beteiligten den Aufwand und schützen Bürger_innen, Gemeinden und die Gemeinderatsmitglieder selbst. Auf unserer Webseite bieten wir darüber hinaus regelmäßig Informationen, die für Gemeinden von Interesse sind, und werden künftig auch verstärkt kommunalspezifische Themen etwa in unserem Newsletter aufgreifen.

Erteilung personenbezogener Informationen über Grundstücke durch Kommunen

Immer wieder erreichen uns Anfragen dazu, ob und – wenn ja – unter welchen Voraussetzungen Gemeinden Privatpersonen oder Firmen Auskunft über den Eigentümer oder die Eigentümerin eines Grundstücks erteilen dürfen. Dabei gilt wie immer unter Jurist_innen: Es kommt drauf an. Oder anders: Entscheidend sind die Voraussetzungen der jeweiligen Rechtsgrundlage.

Aus unterschiedlichen Gründen kommt es vor, dass jemand von einer Gemeinde personenbezogene Informationen über Grundstücke erlangen möchte, beispielsweise wissen will, wer Eigentümer_in eines bestimmten Grundstücks ist: Dies kann beispielsweise ein Landwirt sein, der ein Kaufinteresse an einem unbebauten Nachbargrundstück hat, oder eine Firma, die Windenergieanlagen errichten und zu diesem Zweck geeignete Grundstücke erwerben oder pachten möchte. Bereits eine Kontaktaufnahme zu dem Grundstückseigentümer der Eigentümerin ist regelmäßig in diesem Fall nur dann möglich, wenn dessen oder deren Identität bekannt ist. Zur Beantwortung der Frage, ob eine Gemeinde diese Information übermitteln darf, ist zunächst entscheidend, aus welchem Kontext die Information gewonnen werden soll. Dies gibt wiederum Aufschluss darüber, welches Gesetz eine Rechtsgrundlage für die Übermittlung enthalten könnte.

Denkbar ist beispielsweise, dass die begehrte Information dem Bauamt vorliegt, weil eine Grundstückseigentümerin erst kürzlich einen Antrag auf Baugenehmigung gestellt hat. Hier könnte etwa eine Nachbarin oder ein Nachbar über Bauvorhaben auf dem angrenzenden oder sonst benachbarten Grundstück zu informieren sein. Hierfür enthalten die Regelungen aus § 55 Abs. 1 der Landesbauordnung (LBO) in Verbindung mit § 4 des Landesdatenschutzgesetzes (LDSG) die einschlägige Rechtsgrundlage. Daneben kommen weitere Rechtsgrundlagen aus dem Bau- und allgemeinen Verwaltungsrecht in Betracht, wie z. B. die Aktenauskunft nach § 29 Landesverwaltungsverfahrensgesetz (LVwVfG). Vereinfacht gesagt, wird hier die Information aber immer dann nicht möglich sein, wenn die anfragende Person von dem baurechtlichen Verfahren nicht berührt ist. Ein reines Kaufinteresse wäre in diesem Zusammenhang daher grundsätzlich nicht ausreichend, die Informationsübermittlung zu rechtfertigen.

Die Information, wem welches Grundstück gehört, wird auch den kommunalen Finanzämtern bekannt sein, da sie für die Erhebung der Grundsteuer zuständig sind. Allerdings gilt hier das Steuergeheimnis, so dass eine Preisgabe dieser Informationen nur in seltenen Fällen zulässig ist, vgl. § 30 Abga-

benordnung (AO) und für eine etwa erforderliche Zweckänderung § 29c AO. Ein reines Kaufinteresse gehört jedenfalls nicht dazu.

Die Eigentümer_inneneigenschaft ließe sich auch dem Grundbuch entnehmen: Gem. § 12 Abs. 1 der Grundbuchordnung (GBO) ist jeder_m die Einsicht in das Grundbuch gestattet, die oder der ein berechtigtes Interesse darlegt. Die Grundbücher werden zwar von den Amtsgerichten geführt. Bei vielen Gemeinden in Baden-Württemberg findet sich jedoch eine Grundbucheinsichtsstelle i. S. v. § 149 GBO, § 35a des Landesgesetzes über die freiwillige Gerichtsbarkeit. Deren Aufgaben werden im Wege der Organleihe von einem vom Bürgermeister oder von der Bürgermeisterin bestimmten Ratsschreiber erledigt. Dieser wird insoweit indes als Urkundsbeamte_r der Geschäftsstelle des Grundbuchamts, also des Amtsgerichts, tätig.

Für die eingangs genannten Beispiele wird es letztlich auf die Zulässigkeit einer Auskunft aus dem Liegenschaftskataster ankommen. Das Liegenschaftskataster ist – vereinfacht gesagt – ein Register aus dem Vermessungswesen, welches Aufschluss über die Einteilung und die Beschaffenheit von Grund und Boden gibt, vgl. § 4 Abs. 1 S. 1 des Landesvermessungsgesetzes (VermG). Die darin enthaltenen Geobasisinformationen können auf Antrag auch an Private übermittelt werden. Rechtsgrundlage für die Übermittlung personenbezogener Daten aus dem Liegenschaftskataster ist § 2 Abs. 3 S. 2 VermG: Angaben zu den Grundstückseigentümern und Erbbauberechtigten dürfen nach dieser Vorschrift übermittelt werden, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis dieser Informationen darlegt. Ähnliche Regelungen existieren auch in anderen Bundesländern, siehe etwa § 5 Abs. 2 S. 1 Nr. 2 des Niedersächsischen Gesetzes über das amtliche Vermessungswesen.

Der unbestimmte Rechtsbegriff des „berechtigten Interesses“ wurde vom Gesetzgeber nicht näher erläutert. Unzweideutig dient diese Voraussetzung jedoch dem Schutz des Rechts auf Informationelle Selbstbestimmung. Dies ergibt sich schon aus der Begründung des Gesetzentwurfs, mit dem die Regelung eingeführt wurde. Darin hieß es:

» *Der Zugriff auf diese personenbezogenen Informationen ist […] nur bei einem berechtigten Interesse des Empfängers an diesen Informationen erlaubt […]. Das Recht auf informationelle Selbstbestimmung des Betroffenen wird damit gewährleistet. Der Gesetzgeber konkretisiert mit dieser Regelung eine Ausnahme zu dem Grundsatz, dass Geobasisinformationen als öffentliche Informationen all-*

gemein zugänglich sein sollen. Er nimmt damit einen Ausgleich zwischen den an ein öffentliches Register gestellten Anforderungen und dem Schutz persönlicher Daten vor.« (LT-Drs. 14/7075, S. 28).

Bei der Auslegung des vermessungsrechtlichen „berechtigten Interesses" lehnt sich die Rechtsprechung an die Auslegung des von § 12 Abs. 1 GBO geforderten „berechtigten Interesses" an (vgl. beispielsweise VG Dresden, Urt. vom 6. November 2019 – 4 K 5232/17; VG Würzburg, Urt. vom 26. Februar 2020 – W 6 K 19.411 und VG Hannover, Urt. vom 1. November 2022 – 12 A 4356/20). Demnach genügt sowohl im Bereich des Grundbuchrechts als auch im Bereich des Vermessungsgesetzes grundsätzlich ein verständiges, durch die Sachlage gerechtfertigtes Interesse an der Information. Auch ein tatsächliches, wirtschaftliches oder öffentliches Interesse kann also ein Recht zur Einsichtnahme begründen. Während allerdings die zivilgerichtliche Rechtsprechung für das „berechtigte Interesse" des § 12 Abs. 1 GBO fordert, dass dieses über bloße Kaufinteressen hinausgeht, die auskunftsbegehrende Person also beispielsweise bereits in Vorverhandlungen mit dem_der Eigentümer_in stehen muss, so haben dies die o.g. Gerichte für das Vermessungswesen anders beurteilt: Es bedarf keines bereits bestehenden, konkreten Rechtsverhältnisses zwischen der antragstellenden Person und dem Eigentümer oder der Eigentümerin, Kaufinteressen sind hier grundsätzlich ausreichend. Begründet wird dies mit dem unterschiedlichen Umfang derjenigen Informationen, die sich aus dem Grundbuch und dem Liegenschaftskataster ergeben: Aus dem Grundbuch lassen sich weitergehende Rückschlüsse auf die Vermögensverhältnisse ziehen, insbesondere durch Erkenntnisse zu Belastungen des Grundstücks.

Auch wir gehen davon aus, dass eine Auskunft zur Klärung einer Verkaufsbereitschaft auf § 2 Abs. 2 S. 2 VermG gestützt werden kann und das „berechtigte Interesse" im Sinne der o.g. Rechtsprechung weit auszulegen ist. Gleichwohl weisen wir darauf hin, dass das Interesse ernsthaft und hinreichend konkret sein muss, also beispielsweise gegenüber einer reinen Neugier oder der Verfolgung unbefugter Zwecke abzugrenzen ist. Deswegen muss die antragstellende Person ihr Interesse in angemessenem Umfang gegenüber der Gemeinde darlegen. Außerdem ist der jegliches Verwaltungshandeln bindende Verhältnismäßigkeitsgrundsatz zu berücksichtigen: Sind entgegenstehende Interessen der betroffenen Person bekannt oder ersichtlich, sind diese mit dem berechtigten Interesse in Abwägung zu bringen.

Neben der Prüfung der jeweiligen Rechtsgrundlage sollte die Gemeinde das Vorliegen der Voraussetzungen und die in die Abwägung mit eingeflossenen Erwägungen dokumentieren. Für die Empfängerseite gelten im Übrigen auch die allgemeinen datenschutzrechtlichen Grundsätze, allen voran diejenigen der Zweckbindung und der Transparenz: Betroffene Personen sind also nach Art. 14 DS-GVO zu informieren und die Daten nach Zweckerreichung zu löschen.

Gemeinden können aufgrund verschiedener Rechtgrundlagen Privaten Auskunft über Grundstückseigentümer_innen geben. Entscheidend ist es, den „Herkunftsort" der Information einer Rechtsgrundlage zuzuordnen und das Vorliegen der jeweiligen Voraussetzungen zu prüfen und zu dokumentieren.

Gerne mehr davon: Im Austausch mit dem LfDI

Im Zuge unserer Aufgabe, öffentliche Stellen zu beraten und Verantwortliche für den Datenschutz zu sensibilisieren, sind wir in verschiedenen Formaten mit den öffentlichen Stellen des Landes im Austausch. Ziel ist es, proaktiv mit aktuellen Fragen in Kontakt zu kommen und bei Bedarf zu unterstützen.

In verschiedenen Formaten vertiefen wir unseren Austausch mit den öffentlichen Stellen des Landes und unterstützen die Beschäftigten anderer Häuser bei der Beantwortung datenschutzrechtlicher Fragen. So nehmen wir beispielsweise als Gäste an Besprechungen verschiedener Arbeitskreise teil oder richten solche Foren selbst aus. So haben wir in diesem Jahr im Rahmen einer von der Hochschule der

Bild: Maksym Yemelyakov-stock.adobe.com

Einmal im Monat eine neue Folge, manchmal öfter – der LfDI Podcast „Datenfreiheit".

Polizei ausgerichteten Schulungsveranstaltung mit den behördlichen Datenschutzbeauftragten der Polizeipräsidien über aktuelle Datenschutzfragen diskutiert und im Rahmen des von uns veranstalteten „Forums kommunaler Datenschutz" verschiedene Themen mit den kommunalen Interessensvertretungen besprochen. In solchen Kontexten können Datenschutzfragen niedrigschwellig diskutiert und das gegenseitige Verständnis geschult werden. Ziel ist es, für datenschutzrechtliche Erwägungen frühzeitig zu sensibilisieren und zugleich Einblicke in die praktischen Umsetzungsfragen zu erhalten. In diesem Zusammenhang steht auch unser Angebot, dass behördliche Datenschutzbeauftragte Einblicke in unsere Arbeit erhalten können. Besonders freut es uns, dass – nachdem zwei Kolleginnen unseres Hauses im Jahr 2022 selbst zwei Wochen den Alltag eines kommunalen behördlichen Datenschutzbeauftragten begleitet haben – in Berichtsjahr nun ein polizeilicher Datenschutzbeauftragter zwei Wochen bei uns hospitiert hat. Darüber hinaus bietet unser Bildungszentrum in regelmäßigen Abständen die Schulung „Datenschutzgrundlagen für öffentliche Stellen" an, welche sich auch an Personen mit wenig Vorerfahrung im Datenschutz richtet und grundlegende datenschutzrechtliche Kenntnisse mit Praxisbeispielen vermittelt.

Wir schätzen den kontinuierlichen Austausch mit den anderen öffentlichen Stellen des Landes und freuen uns auch zukünftig auf interessante Diskussionen.

Schnuppertag im Rathaus mit Folgen

Kindern die vielseitige Arbeit der Kommunen näherzubringen, ist toll, aber gar nicht so einfach. Bei einem Schnuppertag wollte eine Stadtverwaltung erklären, was es mit der Hundesteuer auf sich hat, und befragte zur Veranschaulichung die Kinder, wer einen Hund zu Hause habe. Die daraus gezogenen Folgen waren kein Kinderspiel.

Kommunen erfüllen eine Vielzahl an öffentlichen Aufgaben. Oftmals kennen Bürger_innen jedoch kaum die enorme Vielfalt, für die Stadtverwaltungen stehen. Und wo bereits Erwachsene Schwierigkeiten haben, sich die Tätigkeit der Verwaltung vorzustellen, fällt es Kindern noch schwerer: Das abstrakte Aufzählen von Bezeichnungen wie „Abfallwirtschaft", „Liegenschaftsverwaltung" oder „Vermessungswesen" – um ein paar plakative Beispiele zu nennen – wird den wichtigen Beitrag der Kommunen zur öffentlichen Aufgabenerfüllung kaum begreifbar machen.

Im einem Fall im Berichtsjahr war einer Klasse Grundschulkindern im Rahmen eines Besuchstags bei der Stadtverwaltung unter anderem die Hundesteuer erklärt worden. Eine solche müssen Gemeinden in Baden-Württemberg erheben und die Modalitäten dafür in einer gemeindlichen Satzung festlegen (§ 9 Abs. 3 des Kommunalabgabengesetzes [KAG]). Legt sich also jemand mit Wohnsitz in einer Gemeinde einen Hund zu, so muss diese Person der Gemeinde grundsätzlich nach Maßgabe der Satzung eine Steuer auf ihr Tier zahlen. Um zu demonstrieren, wie das Ganze funktioniert, fragte die Stadtverwaltung die Besuchsklasse danach, wer denn einen Hund zu Hause habe. Einige der Schüler_innen wurden herausgegriffen und im entsprechenden Register gezeigt, wie Hund und Familie dort eingetragen sind. Bei einem Kind blieb der Abgleich mit dem Register jedoch ergebnislos: Der Hund war noch nicht angemeldet. Nun – im Anschluss wurde den Eltern des Kindes eine Aufforderung zur Anmeldung des Hundes zugesandt.

Obwohl den zuständigen Behörden der Steuerverwaltung grundsätzlich weitreichende Ermittlungsbefugnisse zustehen und sie im Allgemeinen bei Kenntnis von relevanten Tatsachen auch tätig werden müssen, ist dieses Vorgehen in mehrerlei Hinsicht problematisch.

Die Kommune hatte hier als Finanzbehörde keine Berechtigung dazu, die Information über die Hundehaltung in der Familie auf diese Weise von dem Grundschulkind zu erheben. Zwar können nach den hier anwendbaren allgemeinen steuerrechtlichen Regelungen die Finanzbehörden sowohl von den Beteiligten eines Steuerverfahrens als auch von anderen Personen die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte verlangen (§ 93 Abs. 1 Satz 1 der Abgabenordnung [AO] in Verbindung mit § 3 Abs. 1 Nr. 3 KAG). Dabei sollen allerdings andere Personen als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht (§ 93 Abs. 1 Satz 3 AO in Verbindung mit § 3 Abs. 1 Nr. 3 KAG). In Bezug auf die Hundesteuer ist davon auszugehen, dass der erwachsene Haushaltsvorstand hundesteuerpflichtig war, nicht das Kind. Das Kind wäre demnach nicht nur nachrangig gegenüber den Eltern bzw. dem den Haushalt führenden Elternteil zu befragen gewesen; ihm hätte als Angehörigem der steuerpflichtigen Person(en) vor allem auch ein Auskunftsverweigerungsrecht zugestanden, über das es vorab zu belehren gewesen wäre (§ 101 Abs. 1 AO in Verbindung mit § 3 Abs. 1 Nr. 3 KAG). Bei einem Grundschulkind ist allerdings nicht davon auszugehen, dass es zum Verständnis des Sinns und Zwecks und zur sachgerechten Entscheidung über sein Auskunftsrecht selbst in der Lage wäre, so dass bereits die Belehrung gegenüber dem gesetzlichen Vertreter des Kindes – gegebenenfalls unter Bestellung eines Ergänzungspflegers – hätte erfolgen müssen. Eine ordnungsgemäße Belehrung war mithin hier keinesfalls erfolgt.

Die Erhebung konnte sich hier aber auch nicht unabhängig von den gesetzlichen Erhebungsbefugnissen der Stadtverwaltung auf eine (datenschutzrechtliche) Einwilligung des Kindes stützen. Insoweit kann dahinstehen, ob und inwieweit generell im Steuerrecht mit Blick auf die umfassenden Auskunftspflichten den Finanzbehörden überhaupt eine Erhebung personenbezogener Daten mit steuerlicher Relevanz kraft freiwilliger Einwilligung möglich ist. Auch sei dahingestellt, ob eine Einwilligung seitens des Kindes schon deswegen keine Rechtsgrundlage abgeben kann, weil die Hundehaltung und damit die die Hundesteuerpflicht auslösenden Umstände nicht das Kind, sondern den erwachsenen Haushaltsvorstand betreffen. Ergänzend sei dahingestellt, ob die Stadtverwaltung hier die für eine informierte Einwilligung erforderlichen Informationen erteilt hat. Es lag hier deswegen kei-

Bild: kwasibanane

Es ist datenschutzrechtlich heikel, Kinder bei einem Schnuppertag im Rathaus zu fragen, wer einen Hund daheim hat, und diese Information dann mit der Datenbank abzugleichen.

ne wirksame Einwilligung vor, weil ein Grundschulkind zu jung ist, um eine solche Einwilligung in die Verarbeitung seiner Daten zu erteilen. Auch in Bezug auf die datenschutzrechtliche Einwilligung gilt nämlich, dass ein Grundschulkind deren Tragweite noch gar nicht überblicken kann.

Die Erhebung der Information über die Hundehaltung zum Zwecke des demonstrativen Registerabrufs war mithin rechtswidrig. Doch was bedeutet das für die anschließende Information, dass der Hund der Familie XYZ nicht angemeldet ist? Trotz steuerrechtlichem Untersuchungsgrundsatz ist der Staat bei jeglichem Eingriff in die Grundrechte einer Person an den Grundsatz der Verhältnismäßigkeit gebunden. Er muss also bei der Frage, ob rechtswidrig erlangte Informationen verwertet bzw. auch nur für weitere Erhebungen verwendet werden dürfen, zwischen den verschiedenen Interessen abwägen. Einerseits darf der Staat nicht sehenden Auges doch wegschauen, wenn ihm etwas Rechtswidriges zur Kenntnis gelangt, andererseits darf nicht unberücksichtigt bleiben, wenn von der Rechtsordnung vorgesehene Schutzmechanismen nicht angewendet wurden, wie beispielsweise ein Auskunftsverweigerungsrecht von Angehörigen. Für den Fall der Verletzung der Pflicht zur Belehrung Angehöriger über ihre Auskunftspflicht hat die Rechtsprechung zumindest ein Verwertungsverbot anerkannt (vgl. insbesondere BFH, Urteil vom 31. Oktober 1990 – II R 180/87).

Im hiesigen Fall hatte die Gemeinde vor dem Geschehen keine Überlegungen zu der Erhebung oder Verwend- bzw. Verwertbarkeit von rechtswidrig oder zufällig erlangten Informationen getätigt. Als wir auf die Beschwerde der Eltern des betroffenen Kindes hin die Gemeinde um Stellungnahme baten, hatte diese jedoch bereits begonnen, die interne Vorgehensweise bei den Besuchstagen von Schulkindern zu überarbeiten. Insoweit haben wir vor allem dafür sensibilisiert, dass vor jeder Verarbeitung personenbezogener Daten überlegt werden muss, ob dafür jeweils eine Rechtsgrundlage besteht – und dass allein die Kenntnis über die Rechtswidrigkeit eines Verhaltens nicht ausreicht, um rechtswidrig erlangte Informationen verwerten zu dürfen.

Gerade Kindern gegenüber sollte klar sein, dass staatliches Handeln auf gesetzlicher Grundlage erfolgen muss. Sie nach ihren persönlichen Lebensumständen zu befragen, sollte keine Grundlage zur Einleitung hoheitlicher Verfahren sein.

Neues aus dem Amt: Gesundheits-, Sozial- und Bildungswesen

Beratung zu einem Forschungsprojekt im Bereich der Kinder- und Jugendhilfe

Im Berichtszeitraum haben wir das Universitätsklinikum Ulm und das Landratsamt Tübingen im Rahmen eines Forschungsvorhabens im Bereich der Kinder- und Jugendhilfe beraten. Bei dem Forschungsprojekt geht es um die Aufarbeitung eines Falls von Kindeswohlgefährdung.

Das Forschungsprojekt ist so konzipiert, dass aus den Jugendamtsakten des Landratsamts Tübingen zunächst eine sogenannte Fallgeschichte erstellt werden soll. Die Fallgeschichte, die die Grundlage für die systematische Aufarbeitung des Falls von Kindeswohlgefährdung bildet, soll an eine vom Universitätsklinikum Ulm geleitete Expert_innenkommission übermittelt werden, welche den Fall im Anschluss wissenschaftlich aufarbeitet. Ziel der Aufarbeitung ist es, problematische Strukturen und Prozesse zu analysieren und für die künftige Arbeit in der Kinder- und Jugendhilfe Verbesserungsvorschläge auszuarbeiten.

Auch wenn die Fallgeschichte keine Namen und Anschriften der betroffenen Personen enthalten wird, ist trotzdem nicht bei allen betroffenen Personen ausgeschlossen, dass ein Personenbezug, z. B. mit Zusatzwissen, herstellbar bleibt. Deswegen ist die Weitergabe der Fallgeschichte an die Expert_innenkommission rechtlich gesehen eine Übermittlung von Sozialdaten zu Zwecken der Forschung nach § 75 des Zehnten Buchs des Sozialgesetzbuchs (SGB X).

Sozialdaten – hierbei handelt es sich um personenbezogene Daten, die ein Sozialleistungsträger, z. B. ein Jugendamt, im Rahmen seiner Aufgaben nach dem Sozialgesetzbuch verarbeitet (§ 67 Abs. 2 Satz 1 SGB X) – sind besonders geschützt. Aber auch die Forschungsfreiheit steht unter besonderem Schutz (z. B. durch das Grundgesetz). Aufgabe des Rechts ist es, diese unterschiedlichen Verfassungsgüter in Einklang zu bringen.

Dies wurde in § 75 SGB X dadurch gelöst, dass die Übermittlung von Sozialdaten zum Zwecke der Forschung zwar möglich ist, aber relativ hohen Anforderungen unterliegt. Formal bildet sich dies dadurch ab, dass die Datenübermittlung von der obersten Bundes- oder Landesbehörde genehmigt werden muss, die für den Bereich zuständig ist, aus dem die Daten herrühren. Inhaltlich ist Voraussetzung, dass die Übermittlung von Sozialdaten für das Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich erforderlich sein muss und dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden oder dass das öffentliche Interesse an der Forschung das Geheimhaltungsinteresse der betroffenen Person erheblich überwiegt. Des Weiteren ist eine Einwilligung der betroffenen Person(en) bezüglich der Übermittlung ihrer Sozialdaten einzuholen, soweit dies zumutbar ist.

Ein Punkt unserer Beratung war die Frage, wie die Einwilligungserklärungen konkret zu gestalten sind. Bei Einwilligungserklärungen im Bereich der Forschung ist insbesondere darauf zu achten, dass diese ausreichend bestimmt sind und in informierter Weise erfolgen. Nur dann kann die betroffene Person eine selbstbestimmte Entscheidung darüber treffen, ob sie mit der Datenverarbeitung einverstanden ist oder nicht. In unserem Fall gab es hier Anpassungsbedarf: Auf unsere Empfehlung hin wurde die Einwilligung noch explizit um Zweckangaben ergänzt, also insbesondere um Angaben dazu, was Ziel der Aufarbeitung des Jugendhilfefalls ist. Des Weiteren wurde zur besseren Verständlichkeit genauer erläutert, was eine Fallgeschichte ist bzw. wie diese aus den Akten des Jugendamts erstellt wird.

Weiterer Gegenstand unserer Beratung war der folgende: Unter anderem mangels entsprechenden Personals für die Erstellung einer Fallgeschichte wollte das Landratsamt diese gerne im Wege der Datenverarbeitung im Auftrag erstellen lassen. In

diesem Fall verarbeitet ein weisungsgebundener Auftragnehmer personenbezogene Daten im Auftrag des Landratsamts (bzw. des Jugendamts), welches datenschutzrechtlich Verantwortlicher bleibt. Hier stand zunächst die Frage im Raum, ob die Erstellung der Fallgeschichte überhaupt als Auftragsverarbeitung angesehen werden kann (oder ob es sich hierbei um eine fremde Fachleistung eines eigenständig Verantwortlichen handeln würde). Für den konkreten Fall haben wir die Möglichkeit einer Auftragsverarbeitung im Ergebnis bejaht. Allerdings sollte aus unserer Sicht nicht das Universitätsklinikums Ulm selbst bzw. ein dortiger Mitarbeitender beauftragt werden, da zweifelhaft ist, dass das Universitätsklinikum als forschende Stelle gleichzeitig auch (geeigneter) Auftragnehmer sein kann.

Forschung ist auch mit Sozialdaten möglich. Mit Blick auf die hohe Sensibilität dieser personenbezogenen Daten sind hier aber die besonderen Anforderungen des Sozialgesetzbuchs zu beachten.

Das Gesetz zur Errichtung einer Pflegekammer

Im Berichtszeitraum wurde das „Gesetz zur Errichtung einer Pflegekammer und zur Änderung weiterer Rechtsvorschriften" vom Landtag beschlossen. Beim Gesetzgebungsverfahren wurden wir beteiligt.

Mit dem Gesetz werden die rechtlichen Grundlagen für eine Landespflegekammer geschaffen. Dem Bericht der Enquetekommission „Pflege in Baden-Württemberg zukunftsorientiert und generationengerecht gestalten" zufolge sind wichtige Ziele einer Pflegekammer, dass Pflegende auf Augenhöhe mit den anderen Entscheidenden im Gesundheitswesen agieren können, die Angehörigen der Pflegeberufe in ihrem Selbstverständnis gestärkt werden und die in der Pflege Beschäftigten bei der Weiterentwicklung des Berufsbildes miteinbezogen werden.

Der uns vorgelegte Gesetzentwurf orientierte sich an dem Gesetz über das Berufsrecht und die Kammern der Heilberufe (Heilberufe-Kammergesetz), welches die Berufsausübung, die Berufsvertretungen und die Berufsgerichtsbarkeit der Ärztin_innen, Zahnärzt_innen, Tierärzt_innen, Apotheker_innen und Pschotherapeuth_innen.

Aus datenschutzrechtlicher Sicht war aus unserer Sicht misslich, dass § 4 des Gesetzentwurfs (Melde- und Auskunftspflichten der Mitglieder; Datenverarbeitung durch die Kammer; Verwaltungszusammenarbeit mit Behörden des Herkunfts- und Aufnahmestaates) – eine Vorschrift, die in erheblichem Maße Datenverarbeitungen regelt –, keinerlei Gesetzesbegründung enthielt. Dies ist insbesondere deswegen problematisch, da Eingriffe in das Grundrecht auf informationelle Selbstbestimmung, wie sie in dieser Vorschrift erfolgen, einer tragfähigen Begründung und nachvollziehbaren Abwägung bedürfen.

Inhaltlich hatten wir u. a. bezüglich § 4 Abs. 2 Satz 1 und Satz 2 des Gesetzentwurfs Grund zur Stellungnahme. Die dort vorgesehenen Regelungen lauteten wie folgt:

» *Die Landespflegekammer ist berechtigt, personenbezogene Daten zu verarbeiten, soweit dies für die Wahrnehmung der ihr durch Gesetz oder Rechtsverordnung übertragenen Aufgaben erforderlich ist. Die Landespflegekammer darf personenbezogene Daten nur an andere Stellen übermitteln, soweit dies zur Aufgabenwahrnehmung dieser Stellen erforderlich ist.* «

Hierzu haben wir darauf hingewiesen, dass die in Satz 2 geregelte „Übermittlung" datenschutzrechtlich gesehen ein Unterfall der in Satz 1 genannten „Verarbeitung" ist (vgl. Artikel 4 Nr. 2 DS-GVO). So wie die Regelung gefasst ist, dürfte Satz 2 „Lex specialis" zu Satz 1 sein. Dies wiederum bedeutet, dass eine Übermittlung unter den in Satz 2 genannten Voraussetzungen (zur Aufgabenwahrnehmung anderer Stellen erforderlich) erlaubt wäre, nicht aber zur Aufgabenwahrnehmung der Landespflegekammer selbst.

Da wir Zweifel hatten, dass dies tatsächlich so gewollt bzw. praktikabel ist, haben wir das Sozialministerium um entsprechende Prüfung gebeten.

Im inzwischen vom Landtag beschlossenen Gesetz wurde das Wörtchen „nur" gestrichen. Nun ist eine Datenübermittlung auch zulässig, wann dies für Aufgaben der Pflegekammer selbst erforderlich ist.

Des Weiteren hatten wir kritisiert, dass die Übermittlungsbefugnis in Satz 2 (Die Landespflegekammer darf personenbezogene Daten an andere Stellen übermitteln, soweit dies zur Aufgabenwahrnehmung dieser Stellen erforderlich ist) sehr viel weiter gefasst ist als die entsprechende Übermittlungsbefugnis im Rahmen des Heilberufs-Kammergesetzes, bei der die Befugnis zur Übermittlung auf die Aufgabenwahrnehmung bestimmter, konkret benannter Stellen beschränkt ist. Die im Gesetzentwurf vorgesehene Regelung hätte bedeutet, dass eine Übermittlung (im Rahmen des Erforderlichen) an jede öffentliche oder nicht-öffentliche Stelle in Betracht gekommen wäre. Auch diesbezüglich wurde nachgebessert: Im beschlossenen Gesetz ist eine Übermittlung (zum Zwecke der Aufgabenwahrnehmung der empfangenden Stelle) nur noch an andere Heilberufe-Kammern sowie die Aufsichts- und Berufszulassungskammern zulässig.

Ein weiterer Punkt unserer Stellungnahme: Laut Anschreiben zum Gesetzentwurf sollte eine Wahl zur ersten Vertreterversammlung und damit die Errichtung der Landespflegekammer nur erfolgen, wenn mindestens 60 Prozent der zukünftigen Pflichtmitglieder sich während der Gründungsphase registrieren lassen. Aus dem Gesetzestext zu § 38 Gesetzentwurfs (Errichtung der Landespflegekammer in Baden-Württemberg) ergab sich, dass Einrichtungen, in denen potenzielle Berufsangehörige der Pflegekammer tätig sind, verpflichtet sind, Angaben zu diesen an den Gründungsausschuss zu übermitteln. Allerdings blieb unklar, wie sichergestellt wird, dass eine Registrierung von einer freiwilligen Entscheidung des jeweiligen zukünftigen Pflichtmitglieds abhängig ist und wie das Verfahren der Registrierung durch den Gründungsausschuss abläuft. Da im Rahmen des Registrierungsprozesses personenbezogene Daten verarbeitet werden, haben wir darum gebeten, diesen Prozess im Gesetz genauer zu regeln.

Auch diesbezüglich hat das Sozialministerium Änderungen am Gesetzentwurf vorgenommen. In der Vorschrift, die die Errichtung der Landespflegekammer in Baden-Württemberg regelt (nun § 44), wurde erstens ausdrücklich aufgenommen, dass der Gründungsausschuss berechtigt ist, personenbezogene Daten zu verarbeiten, soweit dies für die Wahrnehmung seiner Aufgaben erforderlich ist. Des Weiteren wird nun etwas genauer ausgeführt, wie die Registrierung erfolgt: Die Wahl zur ersten Vertreterversammlung darf gemäß Abs. 7 nur durchgeführt werden, wenn mindestens 60 Prozent der potenziellen Kammermitglieder vom Gründungsausschuss registriert sind; dabei werden nur Registrierungen berücksichtigt, gegen die keine schriftlichen oder digitalen Einwendungen erhoben wurden, unabhängig davon, ob die Einwendung im Einzelfall „berechtigt" ist (dies ist nach dem Gesetz der Fall, wenn die Voraussetzungen der Pflichtmitgliedschaft nicht vorliegen) oder nicht.

Mehr Infos:

Entwurf des Gesetzes zur Errichtung einer Landespflegekammer und Änderung weiterer Rechtsvorschriften:

beteiligungsportal.baden-wuerttemberg.de/fileadmin/redaktion/beteiligungsportal/gesetzentwuerfe/221221_Gesetzentwurf_Landespflegekammer.pdf

Gesetzesbeschluss des Landtags zum Gesetz zur Errichtung einer Landespflegekammer und zur Änderung weiterer Rechtsvorschriften:

www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP17/Drucksachen/4000/17_4749_D.pdf

Datenschutzkonform – die Arbeit des Landeszentrums für Barrierefreiheit

Die Teilhabe von Menschen mit Behinderung am gesellschaftlichen Leben ist unverzichtbare Voraussetzung für die Schaffung gleichwertiger Lebensbedingungen und einer inklusiven Gesellschaft.

Baden-Württemberg hat ein Kompetenzzentrum für Barrierefreiheit (Landeszentrum für Barriere-

Bild: Robert Kneschke-stock.abobe.com

Die Teilhabe von Menschen mit Behinderung am gesellschaftlichen Leben ist unverzichtbar.

freiheit, LZ-BARR) eingerichtet, das im Dezember 2022 seine Arbeit aufgenommen hat. Dieses berät zum Thema Barrierefreiheit und fungiert zugleich als Schlichtungsstelle für Konflikte. Es berät unter anderem öffentliche Stellen gemäß § 2 des Landes-Behindertengleichstellungsgesetzes (L-BGG) sowie freie gemeinnützige Einrichtungen und Organisationen in Baden-Württemberg zu verschiedenen Aspekten der Barrierefreiheit. An die Schlichtungsstelle können sich insbesondere in Baden-Württemberg lebende Menschen mit Behinderung, deren Angehörige sowie Verbände. Einen Monat vor der geplanten Eröffnung wandte sich das LZ-BARR mit einer Beratungsbitte an uns. Hierbei ergab sich insbesondere die Frage, aufgrund welcher Rechtsgrundlage(n) das LZ-BARR personenbezogene Daten verarbeitet.

Unter anderem plante das LZ-BARR auf seiner künftigen Website ein Kontaktformular einzusetzen, um (Beratungs-)Anfragen bearbeiten zu können sowie Öffentlichkeitsarbeit zu betreiben. Hierbei sollten Name, E-Mail und Anliegen abgefragt werden. Das LZ-BARR wollte diese Datenverarbeitung u. a. auf Artikel 6 Abs. 1 Buchst. e der Datenschutz-Grundverordnung (DS-GVO) stützen. Das Einholen einer Einwilligung der betroffenen Person hielt das LZ-BARR für entbehrlich. Darüber hinaus sollten Menschen mit Behinderungen online über die Webseite des LZ-BARR einen Schlichtungsantrag bei der Schlichtungsstelle stellen können. Im Antragsformular sollten Name, Anschrift, E-Mail, Grad der Behinderung und der Beschwerdesachverhalt abfragt werden. Der Schlichtungsantrag sollte dann von der Schlichtungsstelle an den Antragsgegner mit der Möglichkeit zur Stellungnahme gesendet werden. Einzelheiten zum Ablauf des Schlichtungsverfahrens seien – so das LZ-BARR – in der „Verwaltungsvorschrift des Sozialministeriums über die Verwaltung und Organisation der nichtrechtsfähigen Anstalt des öffentlichen Rechts Kompetenzzentrum für Barrierefreiheit des Landes Baden-Württemberg“ (VwV LZ-BARR) geregelt. Für die Weiterleitung der personenbezogenen Daten – auch der besonders zu schützen-

den Gesundheitsdaten – an die Antragsgegner des Schlichtungsantrags hielt das LZ-BARR die Einholung einer Einwilligung für entbehrlich.

Da die Eröffnung des LZ-BARR unmittelbar bevorstand und sich abzeichnete, dass geplant war, personenbezogene Daten trotz fehlender Rechtsgrundlage zu verarbeiten, banden wir neben dem LZ-BARR direkt auch das Sozialministerium mit ein und teilten das Prüfergebnis mit, das auf Basis der geltenden Vorschriften es derzeit nicht möglich war, das LZ-BARR datenschutzrechtlich rechtmäßig zu betreiben. Durch die Öffnung des LZ-BARR nach außen, d. h. die geplante Aufforderung, sich über die Homepage des LZ-BARR bei Fragen zur und Beschwerden über fehlende Barrierefreiheit an das LZ-BARR zu wenden, war damit zu rechnen, dass das LZ-BARR entsprechende externe Anfragen erreichen werden. Hierbei konnte nicht ausgeschlossen werden, dass bei Anfragen von Bürger_innen, aber auch bei Anfragen oder Stellungnahmen seitens der öffentlichen Stellen personenbezogene Angaben – darunter sogar solche mit besonderen Kategorien personenbezogener Daten i. S. d. Artikel 9 DS-GVO wie namentlich Gesundheitsdaten – mitgeteilt werden. Deren Erhebung und weitere Verarbeitung bedarf jedoch einer Rechtsgrundlage nach Artikel 6 und gegebenenfalls auch nach Artikel 9 DS-GVO.

Die Verarbeitung personenbezogener Daten durch das LZ-BARR konnte nicht auf ein erhebliches öffentliches Interesse (Artikel 6 Abs. 1 Buchst. e DS-GVO i. V. m. § 4 des Landesdatenschutzgesetzes (LDSG) gestützt werden. Hierfür wäre eine (Außen) Rechtsnorm erforderlich gewesen, die die Aufgaben des LZ-BARR ausreichend normenklar regelt. Die Zuständigkeit der öffentlichen Stelle muss nämlich durch Gesetzes- oder zumindest Verordnungs- oder Satzungsrecht zugewiesen werden. Die bis dahin ausschließlich bestehende Regelung der Aufgaben des LZ-BARR durch die VwV LZ-BARR erfüllte – da ihr nicht der Charakter eines wenigstens materiellen Gesetzes zukommt – diese Voraussetzungen nicht.

Insbesondere konnte eine Verarbeitung mangels hinreichender Normenklarheit und Bestimmtheit auch nicht auf Artikel 6 Abs. 1 Buchst. e DS-GVO i. V. m. §§ 7 bis 10 L-BGG a.F. gestützt werden.

Kurz vor Eröffnung des LZ-BARR existierte keine ausreichende Rechtsgrundlage für die beabsichtigten Datenverarbeitungen. Wir rieten dem Sozialministerium daher, sämtliche Verarbeitungen personenbezogener Daten zu unterlassen, soweit diese nicht auf eine informiert und freiwillig (sowie bei besonderen Kategorien personenbezogener Daten: ausdrücklich) erteilte Einwilligung der von der Datenverarbeitung betroffenen Person gestützt sind. Wir machten gegenüber dem Sozialministerium deutlich, dass für den Fall, dass das LZ-BARR berechtigt werden solle, einwilligungsunabhängige Verarbeitungen personenbezogener Daten vorzunehmen, zunächst eine diese rechtfertigende, normenklare gesetzliche Grundlage (im Sinne eines materiellen Gesetzes) zu schaffen wäre.

Für den Fall, dass das LZ-BARR mit seiner Eröffnung Verarbeitungen personenbezogener Daten ohne eine gesetzliche Regelung und ohne eine wirksame Einwilligung vornimmt, kündigten wir an, dass wir aufsichtsrechtlich aktiv werden müssten. Es bestand daher akuter gesetzgeberischer Handlungsbedarf, damit die operative Arbeit des LZ-BARR rechtmäßig erfolgen kann. Dies sah das Sozialministerium nach Eröffnung des LZ-BARR auch und brachte schließlich eine materielle Rechtsgrundlage für das LZ-BARR im L-BGG auf den Weg.

Um die übergangsweise Tätigkeit des LZ-BARR bis zur Verabschiedung einer entsprechenden Neuregelung rechtskonform(er) zu gestalten, wurden unter Berücksichtigung unserer Stellungnahme zahlreiche Maßnahmen seitens des Sozialministeriums ergriffen. Insbesondere wurde die Ausgestaltung des Schlichtungsverfahrens dergestalt angepasst, dass die antragsstellende Person ausdrücklich zur Abgabe einer Einwilligung in die Verarbeitung ihrer personenbezogenen Daten zum Zweck der Durchführung des Schlichtungsverfahrens aufgefordert wurde. Personenbezogenen Daten einer bei der betreffenden öffentlichen Stelle beschäftigten Person wurden im Schlichtungsantrag fortan nicht mehr abgefragt. Innerhalb des Formulars wurde zudem der ausdrückliche und klare Hinweis aufgenommen, keine personenbezogenen Daten Dritter oder Daten, die zur Identifizierung einer konkreten Person führen können, zu übermitteln, da diese nicht

durch das LZ-BARR verarbeitet werden dürften. Ebenso wurde ein erneuter Hinweis aufgenommen, dass auch seitens der öffentlichen Stelle keine personenbezogenen Daten Dritter, wie z. B. die Namen von Mitarbeitenden, genannt werden dürfen. Für den Fall, dass im Rahmen des Schlichtungsverfahrens dennoch personenbezogene Daten übermittelt werden sollten, wurden die Mitarbeitenden des LZ-BARR gesondert dazu verpflichtet, diese Daten sofort zu löschen. Eine Bearbeitung des Antrags würde in diesen Fällen nicht erfolgen.

Binnen zwei Wochen übersandte uns das Sozialministerium den angekündigten Entwurf eines Gesetzes zur Änderung des Landes-Behindertengleichstellungsgesetzes und anderer Gesetze mit der Möglichkeit der Stellungnahme. Im Rahmen dieses Verfahrens wurden all unsere im Vorverfahren geäußerten datenschutzrechtlichen Kritikpunkte und Anmerkungen vollständig umgesetzt. Durch die Einführung neuer Vorschriften ins L-BGG wurde die bis dahin fehlende Rechtsgrundlage für die Arbeit des LZ-BARR und dessen Schlichtungsstelle geschaffen, so dass dessen Betrieb nun rechtmäßig erfolgen konnte.

Die Verarbeitung personenbezogener Daten auf Basis eines erheblichen öffentlichen Interesses oder in Ausübung öffentlicher Gewalt nach Artikel 6 Abs. 1 Buchst. e DS-GVO i. V. m. § 4 LDSG erfordert, dass die Zuständigkeit der öffentlichen Stelle durch Gesetzes- oder zumindest Verordnungs- oder Satzungsrecht zugewiesen werden muss. Die bloße Übertragung einer Aufgabe durch Verwaltungsvorschrift ist hierbei ungenügend.

Gesundheitsdaten und Forschung – weiterhin ein großes Thema

Auch im Berichtsjahr haben wir uns mit dem Thema des Schutzes personenbezogener Daten bei der Forschung auseinandergesetzt, allem voran bei der Forschung mit Gesundheitsdaten. Hier wird schon seit einiger Zeit von Forschenden vorgetragen, dass sie insbesondere zum Zwecke besserer Erkenntnisgewinnung im medizinischen Bereich, einschließlich der Entwicklung und Verwendung von Verfahren der Künstlichen Intelligenz, einen verbesserten, einwilligungsunabhängigen Zugang zu personenbezogenen Gesundheitsdaten benötigen würden. Diese Forderung hat zu einiger gesetzgeberischer Aktivität geführt, sowohl auf europäischer als auch auf nationaler Ebene. Hierzu haben wir die Landesregierung beraten und uns – gemeinsam mit den anderen deutschen Aufsichtsbehörden intensiv in den rechtspolitischen Diskurs eingebracht. Wir haben uns aber auch konkret um die Fragen der Forschenden gekümmert, Fortbildungen für sie angeboten und sie sowie die Landesregierung bei Projekten in diesem Bereich beraten.

Der Europäische Gesundheitsdatenraum

Die europäische Kommission verfolgte mit dem Entwurf einer Verordnung für den europäischen Gesundheitsdatenraum (EHDS) die Ziele, einerseits die Gesundheitsversorgung europaweit zu erleichtern (sogenannte Primärnutzung) und andererseits die Gesundheitsdaten insbesondere für die wissenschaftliche Forschung, aber auch z. B. für Politikgestaltung und Innovation, zu nutzen (sogenannte Sekundärnutzung). Zugleich sollen die Datensätze aus der Gesundheitsversorgung für Maschinelles Lernen zugänglich sein.

☛ Verordnung des Europäischen Parlaments und Rates über den europäischen Raum für Gesundheitsdaten:

eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0197

Der Entwurf wies mit Blick auf den Datenschutz allerdings erhebliche Defizite auf. Um diese aufzuzeigen, haben wir gemeinsam mit den deutschen Aufsichtsbehörden in der „Taskforce Forschungsdaten" der DSK eine Stellungnahme vorbereitet, die sie am 27. März 2023 verabschiedete.

☛ Nutzung von Gesundheitsdaten:

Stellungnahme der Datenschutzkonferenz vom 27. März 2023 „Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen“:

www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf

Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“, vom 24. November 2022:

www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Die Stellungnahme hebt hervor, dass die betroffenen Personen auch hinsichtlich der Verarbeitung ihrer personenbezogenen Daten in einem Gesundheitsdatenraum darauf vertrauen können müssen, dass die Regelungen der DS-GVO und ihre Grundrechte nach Artikel 7, 8 der Charta der Grundrechte der Europäischen Union (GRCh) gewahrt bleiben.

Der Kommissionsentwurf für eine Verordnung zum Europäischen Gesundheitsdatenraum weist im Einzelnen hinsichtlich der Betroffenenrechte, der Normenklarheit und der Bestimmungen zu den technischen und organisatorischen Maßnahmen Defizite auf. Die Datenschutzkonferenz fordert insbesondere eine bessere Einfügung der Regelungen in das Regelungsgefüge der DS-GVO. Auch verlangt sie, die im Gesundheitsdatenraum verarbeiteten Datenkategorien zu begrenzen und hebt sowohl bei der Verarbeitung zur Primärnutzung der Gesundheitsversorgung als auch für die Sekundärnutzung die Souveränität der Patient_innen hervor: Die Patient_innen müssen mit der Datenverarbeitung zu ihrer Gesundheitsversorgung einverstanden sein und müssen auch hinsichtlich der Sekundärnutzung effektive Einwirkungsmöglichkeiten behalten.

☛ Nutzung von Gesundheitsdaten:

Inzwischen haben der Rat am 6. Dezember 2023 und das Europäische Parlament (am 12. Dezember 2023) ihren Standpunkt in Bezug auf den Vorschlag der Kommission für die Verordnung zum Europäischen Gesundheitsdatenraum bezogen, so dass die europäischen Institutionen nunmehr in die Phase des Trilogs eintreten. Dabei haben Rat und Parlament insbesondere den Punkt weitergehender Mitbestimmung der Patient_innen aufgegriffen und schlagen hierzu verschiedene Lösungsmöglichkeiten vor.

www.consilium.europa.eu/de/press/press-releases/2023/12/06/european-health-data-space-council-agrees-its-position

www.europarl.europa.eu/news/de/press-room/20231208IPR15783/personenbezogene-gesundheitsdaten-neue-eu-regelung-fur-verbesserten-zugang

Gesundheitsdatennutzungsgesetz

Mit Blick auch auf die europäischen Entwicklungen im Zusammenhang mit dem Gesundheitsdatenraum hat überdies der Bundesgesetzgeber zur Schaffung von Regelungen für weitergehende Möglichkeiten der Nutzung personenbezogener Gesundheitsdaten Tätigkeit entfaltet. Das damit u. a. verfolgte Anliegen, die wissenschaftliche Forschung zu stärken, erscheint grundsätzlich nachvollziehbar. Aber auch der Entwurf eines Gesundheitsdatennutzungsgesetzes (GDNG) war (neben dem eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens) aus Sicht des Datenschutzes kritisch zu begleiten.

Wir bereiteten daher insbesondere – gemeinsam mit weiteren deutschen Aufsichtsbehörden in der Taskforce Forschungsdaten – eine Stellungnahme zum Entwurf des Gesundheitsdatennutzugsgesetzes vor, die am 3. Juli 2023 von der Datenschutzkonferenz verabschiedet wurde. Diese Stellungnahme kritisierte inhaltliche Ausführungen im Referentenentwurf zu den Pflichten zur Einhaltung der Datenschutzgrundsätze (z. B. durch die Streichung von Speicherhöchstfristen), bestehende Informationspflichten (z. B. durch Regelung zur Erteilung konkreter Informationen nur auf Antrag) und Betroffenenrechte (z. B. durch Verweis auf § 27 Abs. 2 BDSG).

Auch hat die Datenschutzkonferenz die Notwendigkeit nach angemessenen und spezifischen Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen benannt. Bei den spezifischen Maßnahmen zum Datenschutz dürfe sich der Gesetzgeber nicht auf allgemeine Verweise beschränken oder lediglich wiederholen, was nach der Datenschutz-Grundverordnung ohnehin gelte. Auch wiesen wir auf die datenschutzrechtlichen Risiken der Verknüpfung pseudonymisierter Datensätze aus verschiedenen Quellen – insbesondere derjenigen der Daten des Forschungsdatenzentrums mit denen des klinischen Krebsregisters – hin. Denn eine solche Verknüpfung setzt eine konkrete erlaubende Rechtsgrundlage voraus, die strenge Voraussetzungen mit einer Regelung starker technischer Schutzmechanismen erfüllen muss.

Wir forderten in der Stellungnahme einen umfassenden Schutz der Forschung mit Gesundheitsdaten durch ein strafbewehrtes Forschungsgeheimnis. Der Entwurf des Gesundheitsdatennutzungsgesetzes sieht nunmehr solches vor.

☛ **Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 14. August 2023**

zum Referentenentwurf des Bundesministeriums für Gesundheit: Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 3. Juli 2023):

www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf

Darüber hinaus sah der Referentenentwurf eines Gesundheitsdatennutzungsgesetzes mit dem Stand von Anfang Juli 2023 eine grundlegende Änderung im Zuständigkeitsgefüge der deutschen Datenschutz-Aufsichtsbehörden vor: Dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sollten weitreichende Zuständigkeiten zukommen, die bislang den Datenschutz-Aufsichtsbehörden der Länder unterlagen. Insbesondere sollte er die Aufsicht über alle Kranken- und Pflegekassen und die Kassenärztlichen Vereinigungen sowie über alle „Stellen, die gesundheitsbezogene Sozialdaten im Sinne des § 67 SGB X verarbeiten", über registrierte Ethik-Kommissionen im Sinne des § 41a Abs. 1 des Gesetzes über den Verkehr von Arzneimitteln (AMG) sowie über Prüfstellen erhalten, wenn und soweit sie klinische Prüfungen im Sinne des § 4 Abs. 23 AMG durchführen. Hintergrund dieses Regelungsbestrebens war es wohl, dass sich insbesondere Forschende zuweilen beklagen, sich bei länderübergreifenden Forschungsvorhaben mit mehreren Aufsichtsbehörden befassen zu müssen. Wie wir gemeinsam mit den anderen Aufsichtsbehörden der Länder in einer Stellungnahme vom 10. August 2023 darlegten, verstieß die vorgesehene Regelung dabei indes gegen verfassungsrechtliche Vorgaben einschließlich des mit der DS-GVO verfolgten Ziels einer effektiven Datenschutzaufsicht (Kapitel IV DS-GVO): Abgesehen von Unschärfen, die der Regelungsentwurf enthielt und die zahlreiche Unklarheiten in Bezug auf die zuständige Aufsichtsbehörde geschaffen hätten, begründete die geplante Reduktion von 18 auf eine datenschutzrechtliche Aufsichtsbehörde die Gefahr des Rückgangs der aufsichtsbehördlichen Kontrolldichte; außerdem würden sowohl die betroffenen Personen als auch die Nutzenden der Gesundheitsdaten eine „Datenschutz-Aufsichtsbehörde vor Ort" verlieren.

Im Kabinettsentwurf des Gesundheitsdatennutzungsgesetzes vom 30. August 2023 war diese Zuständigkeitsregelung nicht mehr enthalten. Die vorhandene Zuständigkeitsstruktur der Datenschutz-Aufsichtsbehörden auf Landes- und Bundesebene bleibt damit erhalten und erfährt im Zusammenhang mit länderübergreifenden Forschungsvorhaben eine differenzierte Regelung mit der sich die federführende Datenschutz-Aufsichtsbehörde bestimmen lässt, vgl. § 5 Entwurf des Gesundheitsdatennutzungsgesetzes. Eine solche Regelungsstruktur ermöglicht eine den Besonderheiten der Forschungsvorhaben gerecht werdende effektive datenschutzrechtliche Aufsicht und Beratung. Inzwischen sind sowohl das Gesundheitsdatennutzungsgesetz als auch das Gesetz zu vom Bundestag beschlossen worden.

☛ Stellungnahme der unabhängigen Datenschutzaufsichtsbehörden der Länder vom 10. August 2023

zu Artikel 5 des Referentenentwurfs eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 3. Juli 2023): www.datenschutzkonferenz-online.de/media/st/23_08_10_Datenschutzaufsicht-Laender-zu-Art_5_GDNG-E.pdf

Digital-Gesetz – DigiG – des Bundes: www.bundestag.de/dokumente/textarchiv/2023/kw50-de-digitalisierung-gesundheitswesen-980632

Harmonisierung der Forschungsklauseln in den Regelungen des Bundes und der Länder

Dem Bedürfnis der Forschenden nach weniger Komplexität bei den datenschutzrechtlichen Regelungsregimen etwa in Bezug auf länderübergreifende Forschungsvorhaben ist unseres Erachtens unbedingt nachzukommen: Die Regelungen des Bundes und der Länder sollten besser aufeinander abgestimmt werden, idealerweise sollten sie etwa nach dem Vorbild der Verwaltungsgesetze des Bundes und der Länder (oder anderer vergleichbar harmonisierter Gesetze) gleichlautend abgefasst werden. Dies könnte einerseits die Rechtsanwendung der Forschungseinrichtungen vereinfachen, Hürden abbauen und die Forschung stärken, andererseits aber auch ein insgesamt hohes Datenschutzniveau garantieren. Diesen Weg – und Eckpunkte für die zu vereinheitlichenden Regelungen – zeigte die Datenschutzkonferenz mit einer weiteren Entschließung vom 23. November 2023 auf, die wir ebenfalls intensiv mit vorbereiteten.

☛ Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 23. November 2023:

Datenschutz in der Forschung durch einheitliche Maßstäbe stärken: www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

Gesetzliche Regelung medizinischer Register

Aus dem Bereich der medizinischen Forschung ist schließlich noch auf eine weitere Entschließung der Datenschutzkonferenz aus dem Berichtsjahr hinzuweisen: Mit Entschließung vom 23. November 2023 gibt die Datenschutzkonferenz Empfehlungen für die gesetzliche Regulierung medizinischer Register. Anknüpfend an ihre Ausführungen in der Petersberger Erklärung vom 24. November 2022 empfiehlt die Datenschutzkonferenz die Schaffung einer Zentralstelle für medizinische Register als unabhängige Körperschaft des öffentlichen Rechts, die ein Registerverzeichnis führen und die eine Auditierung und Zuordnung medizinischer Register je nach vorhandener Qualitätsstufe verantworten soll. Der Zentralstelle solle zugleich eine besondere Funktion als Ansprechpartnerin und Lotsin für die betroffenen Personen sowie bei der Durchsetzung ihrer Betroffenenrechte zukommen. Darüber hinaus zeigt die Datenschutzkonferenz in ihrer Entschließung datenschutzrechtliche Rahmenbedingungen für eine gesetzliche Regulierung medizinischer Register auf.

☛ Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 22./23. November 2023:

Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register: www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

Beratung des LfDI zu Forschungsprojekten

Wir haben uns unmittelbar den Forschenden zugewandt, um ihnen den Umgang mit datenschutzrechtlichen Fragestellungen im Rahmen ihrer Forschungstätigkeiten zu erleichtern, und die Landesregierung bei forschungsunterstützenden Projekten beraten.

Wir haben – neben verschiedenen Vorträgen zur Thematik – insbesondere eine sehr nachgefragte Fortbildung zu Forschung und Datenschutz über das Bildungszentrum BIDIB angeboten. Auch bei

unserer KI-Woche nahm die Forschung mit Gesundheitsdaten einen prominenten Raum ein.

Darüber hinaus setzten wir unsere beratende Mitwirkung im Forum Gesundheitsstandort Baden-Württemberg fort und erörterten etwa mit der Landesgesellschaft BIOPRO Baden-Württemberg GmbH und dem Ministerium des Inneren für Digitalisierung und Kommunen Baden-Württemberg verschiedene Anwendungsfälle für die Forschung, sogenannte Use Cases. Auch führten wir in diesem Zusammenhang unsere Start-up-Beratung weiter. Wir verfolgten außerdem den Projektauftakt des vom Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg geförderten Projekts ROUTINE im FZI Forschungszentrum Informatik in Karlsruhe, das das Ziel verfolgt, ein Reallabor „KI im Gesundheitswesen" zu begründen. In einem beratenden Auftaktgespräch der Projektpartner mit unserer Behörde haben wir relevante datenschutzrechtlichen Weichenstellungen für eine datenschutzkonforme Projektumsetzung aufgezeigt.

Überdies nahmen wir am Beirat zum Vorprojekt Medi:cus BW teil und berieten in diesem Zusammenhang das Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg. Bei diesem Projekt unter Führung des Innenministeriums und unter Beteiligung weiterer Ministerien geht es darum, die Möglichkeiten auszuloten, eine cloudbasierte Gesundheitsdateninfrastruktur für Baden-Württemberg zu schaffen, die u. a. als standardisierte Datenaustauschplattform, als Plattform für Telekonsultationen und Telekonsile und als Plattform zur (auch einrichtungsübergreifenden) Forschung mit Gesundheitsdaten dienen könnte.

Am Rande erwähnt sei an dieser Stelle auch unsere beratende Unterstützung des Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg bei einem ähnlichen Cloudprojekt, nämlich der Schaffung einer einheitlichen (cloudbasierten) Fachanwendungslandschaft für die Gesundheitsämter, auch wenn dieses Projekt die Forschung nicht schwerpunktmäßig betrifft.

Wir gehen davon aus, dass wir unsere Beratungsleistungen in diesen Projekten auch im kommenden Jahr fortsetzen: Die zahlreichen und verschiedenartigen Forschungsfragen, unsere vielseitige Forschungslandschaft, die Bedeutung der Gesundheitsforschung für die Gesundheitsvorsorge und die Gesundheitsversorgung einschließlich ihrer wirtschaftlichen Dimensionen und der intensiven gesetzgeberischen Aktivitäten lassen insgesamt auch in Zukunft einen hohen Beratungsbedarf bei den unserer Aufsicht unterliegenden Stellen erwarten. Diesen werden wir im Rahmen unserer Kapazitäten gerne nachkommen.

Die Beteiligung des LfDI an Gesetzgebungsverfahren am Beispiel der Änderung des Schulgesetzes

Einer der größeren und datenschutzrechtlich besonders bedeutenden gesetzgeberischen Maßnahmen, an denen wir im Berichtsjahr beteiligt waren, stellte unsere Beteiligung durch das Kultusministerium an der Vorbereitung der Novellierung des Schulgesetzes dar, auf die wir hier wegen des Umfangs unserer Beteiligung näher eingehen wollen.

☛ Änderung der VwV Regelungen im Jahr 2023

Betrifft ein landesrechtliches Regelungsvorhaben (etwa durch Gesetz, Verordnung, Verwaltungsvorschrift – VwV) die Verarbeitung personenbezogener Daten, ist der LfDI zu konsultieren (Art. 36 Abs. 4 DS-GVO, Art. 28 Abs. 2 JI-Richtlinie; § 26 Abs. 2 LDSG, § 89 Abs. 2 PolG). Die Abläufe normiert die „VwV der Landesregierung und der Ministerien zur Erarbeitung von Regelungen". Diese wurde im Berichtsjahr – unter unser Beteiligung – geändert. Erfreulich: Wir sind jetzt schon gleichzeitig mit den betroffenen Ministerien einzubeziehen. Und mehrfach wird auf unser Beratungsangebot bei der Abfassung von solchen Normen hingewiesen. Wir zeichnen die Regelungsentwürfe allerdings nicht mit und haben keine Aufsichtsbefugnisse zur Durchsetzung unserer Hinweise.

VwV Regelungen: www.landesrecht-bw.de/perma?a=-VVBW-IM-20230629-SF

☛ Prüfung von Regelungsentwürfen durch den LfDI

Der LfDI prüft vorwiegend, ob die Regelungsentwürfe – soweit die Verarbeitung personenbezogener Daten betroffen ist – mit höherrangigem Recht (insbesondere mit der DS-GVO/JI-Richtlinie und dem innerstaatlichen Verfassungsrecht) vereinbar sind. Auf Ebene des Verfassungsrechts sind dabei u. a. von zentraler Bedeutung

- das Prinzip der Normenklarheit: Die von Rechtsvorschriften möglicherweise Betroffenen müssen dem Wortlaut der Vorschriften entnehmen, unter welchen Voraussetzungen die Vorschriften inwieweit gelten und welche Rechtsfolgen das hat, und daran ihr Verhalten ausrichten können (s. hierzu z. B. www.bundestag.de/resource/blob/822430/731fb9782ae96f8f6bdbcc-ce38782b29/WD-3-290-20-pdf-data.pdf);
- die Wesentlichkeitstheorie des BVerfG: Der parlamentarische Gesetzgeber muss im Bereich der Grundrechtsausübung die der staatlichen Gestaltung offenliegende Rechtssphäre selbst abgrenzen und darf dies nicht etwa dem Handeln der Verwaltungsbehörde überlassen (s. jüngst BVerfG, Urt. vom 22. November 2023 – 1 BvR 2577/15 u. a. www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/11/rs20231122_1bvr257715.html, Rn. 69).

Positiv ist hervorzuheben, dass uns das Kultusministerium im Rahmen der Erstellung des Entwurfs eines Gesetzes zur Änderung des Schulgesetzes für Baden-Württemberg und des Landespflegegesetzes (s. LT-Drs. 17/5610 vom 19. Oktober 2023) frühzeitig beteiligt und uns sogar Gelegenheit zu einer Erörterung per Videokonferenz gegeben hat. Durch unsere Beratung hat das Kultusministerium seinen Entwurf aus unserer Sicht in vielerlei Hinsicht verbessern können. Hinzuweisen ist insoweit beispielsweise auf die Regelung in § 38 Abs. 6 Satz 2 Schulgesetz (neu). Dieser lautete im Ausgangsentwurf zunächst: „Sie [= die Lehrkräfte] setzen zur Erfüllung des Erziehungs- und Bildungsauftrags auch informationstechnisch gestützte Systeme ein." Unabhängig von unserer weiteren Kritik an dieser Regelung (s. hierzu LT-Drs. 17/5610, S. 91), namentlich an dem Fehlen eines Hinweises, dass die jeweilige Datenverarbeitung zur Erfüllung der Aufgaben erforderlich und angemessen sein muss, haben wir darauf hingewiesen, dass unseres Erachtens nach wie vor nicht die einzelne Lehrkraft datenschutzrechtlich verantwortlich sein sollte, sondern die Schule, und deswegen die Schule die Zwecke und Mittel der Verarbeitung zu bestimmen habe. Es müsse daher zum Ausdruck kommen, dass die Lehrkräfte nur solche Dienste einsetzen dürften, die der Kontrolle der Schule unterlägen und entsprechend von ihr geprüft und freigegeben seien, ggf. unter Abschluss notwendiger Auftragsverarbeitungsverträge. Das Kultusministerium ist diesen Hinweisen nachgekommen und hat sowohl in den Gesetzestext den Passus „im Rahmen der vorhandenen Ausstattung der Schule" eingefügt als auch in der Gesetzesbegründung nähere Klarstellungen zur datenschutzrechtlichen Verantwortung im Sinne von Art. 4 Nummer 7 DS-GVO vorgenommen (LT-Dr. 17/5610, S. 26 und 39).

Zum Teil haben unsere Hinweise zwar nicht – was grundsätzlich die bessere Lösung wäre – zu Klarstellungen im Gesetzeswortlaut geführt, aber immerhin zu klärenden Ausführungen in der Gesetzesbegründung. Diese ist für die Praxis – die Rechtsunterworfenen ebenso wie die Rechtsanwendenden wie z. B. die Schulen – zwar nicht so leicht auffindbar wie der Gesetzestext selbst. Gerade bei Änderungsgesetzen ist es zuweilen sehr mühsam, das maßgebliche Gesetz, das zur aktuellen Fassung des Gesetzestextes geführt hat, herauszufinden und sodann den zugehörigen Gesetzentwurf nebst Begründung aufzufinden. Die Gesetzesbegründung stellt gleichwohl für die rechtliche Praxis ein wichtiges Hilfsmittel dar, um die Einschätzung derjenigen nachzuvollziehen, die den Entwurf verfasst haben; sie ist damit aus juristischer Sicht ein wesentliches Auslegungskriterium. Als Beispiel dafür, dass unsere Hinweise Eingang in die Gesetzesbegründung gefunden haben, kann etwa unsere Anmerkung zu den Regelungen über den sogenannten Notenschutz (§ 89 Abs. 2 und Abs. 3 SchulG-E) angeführt werden. Beim Notenschutz geht es darum, dass bei Schüler_innen mit einer Beinträchtigung von den allgemeinen Prüfungsmaßstäben zum Ausgleich beeinträchtigungsbedingter Nachteile ausnahmsweise abgewichen werden kann, indem bestimmte Leistungsbereiche nicht bewertet werden. Nach einer jüngeren Entscheidung des Bundesverfassungs-

gerichts (BVerfG, Urteil vom 22. November 2023 - 1 BvR 2577/15, 2578/15 und 2579/15) kann es in diesen Fällen zur Herstellung der Chancengleichheit geboten sein, das Abweichen vom Prüfungsmaßstab durch einen Vermerk im Zeugnis kenntlich zu machen. Das Kultusministerium hat deswegen in § 89 Abs. 2 und 3 SchulG-E hierzu eine Verordnungsermächtigung bzw. eine Ermächtigung der Schulleitungen zur Regelung in der Schulordnung aufgenommen. In unserer Stellungnahme haben wir – neben anderen Anmerkungen – darauf hingewiesen, dass unseres Erachtens die Regelungen nicht dazu ermächtigen, Gesundheitsdaten im Sinne von Art. 9 DS-GVO zu verarbeiten. Diesem Hinweis ist das Kultusministerium insoweit gefolgt, als es die hilfreiche Klarstellung in die Begründung des Gesetzentwurfs aufgenommen hat, dass die Gewährung von Maßnahmen zum Notenschutz ohne Angabe der zugrundeliegenden (gesundheitlichen) Beeinträchtigungen im Zeugnis auszuweisen sei. Insofern dürften dem Zeugnis keine konkreten Gesundheitsdaten zu entnehmen sein, die Anlass für eine Benachteiligung auf dem Arbeitsmarkt geben könnten (LT-Drs. 17/5610, S. 28).

Rechtssicherer Einsatz digitaler Lehr- und Lernformen

In Bezug auf andere Regelungen wurden die Hinweise unserer Dienststelle unseres Erachtens leider weniger gut umgesetzt. Auch hierzu zwei Beispiele:

Die Regelung des § 115b Abs. 9 SchG lautete im Gesetzentwurf der Landesregierung (dort Artikel 1 Nummer 13):

» *Das Anwenden automatisierter, anpassungsfähiger Verfahren ist zum Zweck der technischen Unterstützung und Förderung des individuellen Lernweges nach der Rechtsverordnung nach Abs. 11 in ihrer jeweils geltenden Fassung zulässig. Abs. 6 findet entsprechende Anwendung.* «

In der Begründung dazu wird im Gesetzentwurf der Landesregierung (dort die Einzelbegründung zu Artikel 1 Nummer 13) ausgeführt:

» *Automatisierte adaptive Lehr- und Lernformen nach Abs. 9 können als Teil digitaler Lehr- und Lernformen im Rahmen des Unterrichts eingesetzt werden. Automatisierte adaptive Lehr- und Lernformen sind IT-Verfahren, welche die personalisierte und flexible Lernerfahrung von Schülerinnen und Schülern ermöglichen, sich an den individuellen Bedürfnissen und Kompetenzen der Schülerinnen und Schüler ausrichten und auf den Lerndaten der Schülerinnen und Schüler basieren, um darauf aufbauend eine passgenaue differenzierte oder individualisierte Förderung zu ermöglichen.*
Automatisierte adaptive Lehr- und Lernformen dürfen keine auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung im Sinne von Artikel 22 DS-GVO zur Folge haben. Sie unterstützen Schülerinnen und Schüler bei der Verbesserung des individuellen Kenntnis-, Wissens- und Lernstands und fördern selbstorganisiertes Lernen. Die Verarbeitung dieser Daten für eine automatisierte Leistungsbewertung ist unzulässig.
Abs. 9 in Verbindung mit Abs. 6 enthält die Rechtsgrundlage zur Verarbeitung personenbezogener Daten zur Durchführung automatisierter, anpassungsfähiger Lehr- und Lernformen nach Artikel 6 Abs. 1 Satz 1 Buchst. e DS-GVO. «

Der Hinweis auf Art. 22 DS-GVO ist durchaus begrüßenswert. Allerding ist datenschutzrechtlich bedeutsam nicht erst, dass – wie in der Einzelbegründung angesprochen – automatisierte adaptive Lehr- und Lernformen keine auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung im Sinne von Artikel 22 DS-GVO zur Folge haben dürfen und dass die Verarbeitung dieser Daten für eine automatisierte Leistungsbewertung unzulässig ist.

Vielmehr ist bereits datenschutzrechtlich bedeutsam, dass automatisierte adaptive Lehr- und Lernformen „sich an den individuellen Bedürfnissen und Kompetenzen der Schülerinnen und Schüler ausrichten und auf den Lerndaten der Schülerinnen und Schüler basieren“ und damit personenbezogene Daten verarbeiten, die insoweit Profile der Schüler_innen darstellen dürften. Der Entwurf lässt insoweit nicht hinreichend normenklar erkennen, um welche Maßnahmen des Verarbeitens personenbezogener Daten und damit Grundrechtseingriffe es hier inwieweit konkret gehen soll.

Nach der Begründung zur Schulgesetznovellierung sollte insgesamt der rechtssichere Einsatz digitaler Lehr- und Lernformen ermöglicht werden (s. LT-Drs. 17/5610, S. 15), und zwar auch insoweit, als diese digitalen Formen den an sich als Regel vorgesehenen Präsenzunterricht ausnahmsweise ersetzen sollen.

Die zentrale Norm, mit der dies erreicht werden soll, ist dabei die neu eingefügte Regelung in § 115b SchG-E, in Bezug auf den Präsenzunterricht ersetzende Maßnahmen insbesondere Abs. 2–8 und 10–12. Mit Blick auf zahlreiche Unklarheiten in den Formulierungen des Entwurfs, auf die wir das Kultusministerium wiederholt aufmerksam machten (s. zuletzt unsere Stellungnahme in LT-Drs. 17/5610, S. 99ff.), dürfte das Ziel der Rechtssicherheit in verschiedener Hinsicht nicht erreicht werden.

In diesem Kontext steht § 115b Abs. 6 Satz 3 SchG, wonach Schüler_innen sowie Lehrkräfte verpflichtet sind,

» *personenbezogene Daten, einschließlich Ton-, Bild- und Videodaten, durch Schulen verarbeiten zu lassen, soweit dies zur Durchführung des digitalen Lehr- und Lernformats und zur Erreichung der Lernziele in der jeweiligen Unterrichtssituation förderlich und verhältnismäßig ist.* «

Die Formulierung, die Personen seien verpflichtet, verarbeiten zu lassen, ist nicht ganz klar: Soll hier eine Duldungspflicht angeordnet werden – wofür der Wortlaut „lassen" spricht – oder eine Handlungspflicht, etwa einen PC mit Mikro und Kamera anzustellen? Problematisch ist die Erhebung von personenbezogenen Bild- und Ton-Daten durch die Schule, etwa im Rahmen einer Videokonferenz, weil das häusliche Umfeld der Schüler_innen über das Grundrecht der Unverletzlichkeit der Wohnung (Art. 13 des Grundgesetzes [GG]) zusätzlich geschützt ist. Dies adressiert § 115b Abs. 12 SchG ausdrücklich.

Der Eingriff mag abgemildert werden, wenn eine technische Verschleierung des Bildes um die sprechende Person herum vorgenommen wird. Auch die Übertragung von Ton aus dem häuslichen Umfeld stellt aber einen Eingriff dar, insbesondere

Bild: Suzi Mediastock-adobe.com

Digitaler Unterricht.

Unsere Fortbildungsreihe „Schule digital“

https://lfdi-bw.de/schule-digital

auch dann, wenn wegen enger räumlicher Verhältnisse sich die Übertragung von solchen Geräuschen oder Tönen nicht verhindern lässt, die von weiteren Mitbewohnenden erzeugt werden. Wegen der engen Eingriffsvoraussetzungen aus Artikel 13 Abs. 7 GG dürfte dieses Szenario demnach nur dann zu rechtfertigen sein, wenn die Teilnahme von zu Hause aus freiwillig erfolgt.

Der LfDI wird weiterhin seine Rolle der Beratung der Landesregierung bei Regelungsentwürfen engagiert wahrnehmen mit dem Ziel der Schaffung datenschutzkonformer und insbesondere normenklarer Regelungen für das Land Baden-Württemberg. Mit Blick auf das Schulgesetz und dessen Umsetzung wird er insbesondere das Kultusministerium bei der Schaffung der nach der inzwischen erfolgten Verabschiedung des „Gesetzes zur Änderung des Schulgesetzes für Baden-Württemberg und des Landespflegegesetzes“ (GBl. 2023, Nr. 21 vom 8. Dezember 2023, S. 437ff.) anstehenden Rechtsverordnungen und der sonstigen untergesetzlichen Regelungen weiterhin gerne und umfassend beraten.

Nachlese bei Schulen nach Corona

Während der Pandemie wurden in Schulen einige spezielle Datenverarbeitungen zur Pandemiebekämpfung zulässig. Beispielsweise konnten Schüler_innen auf Antrag von der Pflicht zum Besuch des Präsenzunterrichts befreit werden, wenn durch die Vorlage einer ärztlichen Bescheinigung glaubhaft gemacht werden konnte, dass im Falle einer Erkrankung an Covid-19 mit einem besonders schweren Krankheitsverlauf für die Schülerin oder den Schüler oder eine mit ihr oder ihm in häuslicher Gemeinschaft lebende Person zu rechnen war (§ 1 Abs. 3 Corona-Verordnung Schule – CoronaVO Schule – vom 23. November 2022).

Weiter haben die Einrichtungen gegebenenfalls selbst Testungen durchgeführt bzw. Ergebnisse von Testungen anderer verarbeitet (§ 2 CoronaVO Schule vom 4. Juni 2021). Das Aufbewahren von Testergebnissen und von Eigenbescheinigungen (§ 2 Abs. 3 Nr. 2b CoronaVO Schule vom 4. Juni 2021) sowie von ärztlichen Bescheinigungen zur Befreiung vom Präsenzunterricht hat sich nunmehr erübrigt.

Ebenso müssen Impfnachweise oder Unterlagen zu Zutrittsverboten für Schüler_innen, Lehrkräfte und sonstige Personen im Sinne des § 10 Corona-VO Schule vom 13. September 2021 nicht mehr verwahrt werden.

Darüber hinaus wurden während der Pandemie von den Schulen vielfach Informationen zur Unzumutbarkeit des Tragens einer Maske erhoben und gespeichert (§ 3 Abs. 2 Corona-Verordnung – CoronaVO – in Kraft bis zum 1. März 2023). Nach Aufhebung der Maskenpflicht dürfte auch insoweit jede Rechtsgrundlage zur weiteren Verarbeitung entfallen sein. Eine weitere Speicherung und Verarbeitung der genannten personenbezogenen (Gesundheits-) Daten aus den oben genannten Maßnahmen ist nicht mehr notwendig. Folglich sind die Daten zu löschen, vgl. Artikel 17 Abs. 1 Buchst. a DS-GVO.

Nachdem alle aufgezählten pandemiebedingten Verarbeitungen nicht mehr erforderlich sind, schrieben wir im Sommer 2023 stichprobenartig 17 Schulen in Baden-Württemberg an, um nach dem Stand dieser Verarbeitungen bzw. nach deren Löschung zu fragen. Angefragt wurden hier landesweit alle acht Schultypen.

Die Schulen wurden aufgefordert mitzuteilen, ob sie weiterhin auf Grundlage der Corona-Verordnungen erhobene personenbezogene Daten speichern oder anderweitig verarbeiten. Soweit dies der Fall sein sollte, sollten die Schulen insbesondere den Zweck und die Rechtsgrundlage der Verarbeitung mittteilen.

Erfreulicherweise haben alle 17 Schulen auf unsere Anfrage reagiert und erklärt, dass sie keine derartigen personenbezogenen Daten mehr speichern bzw. solche aus der Pandemiezeit stammende personenbezogene Daten gelöscht haben.

Es freut uns, dass sämtliche kontaktierten Schulen bestätigen, dass die pandemiebedingt erhobenen personenbezogenen Daten der Schüler_innen gelöscht wurden.

Bild: kwasibanane

Die Hoffnung ist groß, dass die Pandmie vorbei ist und Coronamasken nicht mehr gebraucht werden, um sich und andere vor dem Coronavirus zu schützen.

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

Neues aus dem Amt: Nicht-öffentliche Stellen

Neues aus dem Bereich Internationaler Datentransfer

Als wichtigste Entwicklung auf dem Gebiet des Internationalen Datentransfers im Berichtszeitraum ist sicherlich die am 10. Juni 2023 in Kraft getretene neue Angemessenheitsentscheidung der Europäischen Kommission für die Übermittlung personenbezogener Daten in die USA, der sogenannte Datenschutzrahmen EU-USA (in englischer Sprache: EU-US Data Privacy Framework (EU-US DPF) zu nennen.

Bekanntlich hat der Europäische Gerichtshof (EuGH) in den Jahren 2015 und 2020 zwei frühere Angemessenheitsbeschlüsse für zertifizierte Stellen in den USA („Safe Harbor" sowie „Privacy Shield") aufgrund unverhältnismäßiger Zugriffsbefugnisse der US-Sicherheitsbehörden und unzureichender Rechtsschutzmöglichkeiten hiergegen für betroffene Personen für ungültig erklärt und damit Datenexporteure in Europa vor Schwierigkeiten gestellt. Nachdem bereits im März 2022 die Präsidentin der Europäischen Kommission und der Präsident der Vereinigten Staaten von Amerika (US-Präsident) eine grundsätzliche Einigung über einen neuen transatlantischen Datenschutzrahmen verkündet hatten, welcher in der Executive Order 14086 durch den US-Präsidenten mündete, nahm die Europäische Kommission den Angemessenheitsbeschluss zum EU-US DPF am 10. Juli 2023 gegen das ablehnende Votum des Europäischen Parlaments an.

Dieser trat am selben Tag in Kraft und ermöglicht seitdem einen Transfer personenbezogener Daten an selbstzertifizierte Stellen in den USA, die auf einer vom US Handelsministerium veröffentlichten Liste verzeichnet sind. Eine Selbstzertifizierung unter dem EU-US DPF steht allen US-Organisationen offen, die der Aufsicht der Federal Trade Commission (FTC) oder des US Department of Transportation (DOT, US-Verkehrsministerium) unterliegen. Von der Aufsichtszuständigkeit der FTC ausgenommen sind insbesondere der Bankensektor, das Versicherungsgewerbe und die Betreiber öffentlicher Telekommunikationsnetze.

Erwähnenswert in Bezug auf den Anwendungsbereich des EU-US DPF ist neben einer „journalistische Ausnahme" für Daten im Zusammenhang mit journalistischer Aktivität und Medienarchiven – diese Daten können nicht auf Grundlage des EU-US DPF übermittelt werden – auch, dass zwar einerseits eine gesonderte (Zusatz-) Zertifizierung für Beschäftigtendaten („Human resources data" – HR-Daten), also Daten die im Beschäftigungskontext übermittelt werden, ermöglicht wurde – kenntlich an dem Eintrag „HR Data" in der Rubrik „Covered Data" beim Eintrag des jeweiligen Datenimporteurs in der EU-US-DPF-Liste – anderseits aber – wie schon bei den vorangegangenen Angemessenheitsentscheidungen – kein einheitliches Verständnis der europäischen und amerikanischen Seite über die Reichweite dieser Zusatzzertifizierung erreicht werden konnte. Obwohl der Begriff „Beschäftigtendaten" durchaus nahelegt, dass darunter zumindest auch die Daten der Beschäftigten des jeweiligen Datenexporteurs – und gegebenenfalls auch anderer Stellen in der EU – fallen, sind damit nach dem Verständnis der US-Seite nur die Daten der Beschäftigten des jeweiligen Datenimporteurs in den USA gemeint.

☛ **EU-US DPF-Liste:**

www.dataprivacyframework.gov/s/participant

www.dataprivacyframework.gov/s

Es ist somit denkbar, dass Exporteure in der EU sich dieses Verständnis zu eigen machen, einen Transfer personenbezogenen Daten ihrer Beschäftigten gestützt auf den EU-US DPF also auch an solche Stellen in den USA vornehmen, die nicht über die Zusatzzertifizierung für Beschäftigtendaten verfügen.

Übermittlungen an Stellen in den USA auf Grundlage geeigneter Garantien gem. Art. 46 DS-

GVO – beispielsweise Standardvertragsklauseln oder Verbindliche Unternehmensrichtlinien (Binding Corporate Rules, BCR) – sind auch weiterhin möglich. Der hierfür nach der Rechtsprechung des EuGH erforderlichen Bewertung der Rechtslage und -praxis in den USA (sog. Transfer Impact Assessment – TIA) können Datenexporteure ab jetzt die von der EU-Kommission im Angemessenheitsbeschluss zum EU-US DPF ausgeführten Bewertungen zugrunde legen und damit nach unserer Auffassung auf das Ergreifen geeigneter zusätzlicher Maßnahmen (sog. „supplementary measures") verzichten. Denn nach Mitteilung der EU-Kommission gelten alle von der US-Regierung im Bereich der nationalen Sicherheit implementierten Schutzmaßnahmen unabhängig von den verwendeten Übermittlungsinstrumenten für alle Datenübermittlungen im Rahmen der DS-GVO an US-Unternehmen.

Verliert der Angemessenheitsbeschluss seine Gültigkeit, müssen Verantwortliche die entsprechenden Übermittlungen auf ein anderes, wirksames Übermittlungsinstrument aus Kapitel V DS-GVO stützen oder die in Rede stehenden Übermittlungen einstellen. Wir haben immer wieder in den vergangenen Jahren darauf hingewiesen, dass ein Angemessenheitsbeschluss Klarheit beim Drittstaatenstransfer in die USA bringen kann, zugleich aber auch auf das Risiko hingewiesen, dass, sofern der Angemessenheitsbeschluss nicht die hohen Standards einhält, die der EuGH formuliert hat in seinen entsprechenden Entscheidungen, eine erneute Klage gegen den Angemessenheitsbeschluss nicht ausgeschlossen ist. Der aktuelle Angemessenheitsbeschluss ist für Datenexporteure sicherlich eine Erleichterung und gibt Sicherheit. Vermutlich ist die Debatte um die Angemessenheit des Beschlusses jedoch nicht beendet.

☛ EU-US DPF

Die Datenschutzkonferenz (DSK) hat umfangreiche Informationen rund um den EU-US DPF in einer Handreichung für Verantwortliche und betroffene Personen zusammengestellt:

datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf

Die Thematik Drittstaatentransfer wird zudem Gegenstand einer ganztägigen Veranstaltung am 21. März 2024 sein, bei dem wir mit hochkarätigen Referent_innen u. a. folgende Themen näher beleuchten wollen: das Schrems II Urteil und seine Folgen, die neue Angemessenheitsentscheidung für die USA, die Standardvertragsklauseln der Kommission, BCR – C und P sowie sonstige Transferinstrumente.

Katzenjammer

Vor einiger Zeit hatten wir einen Hinweis erhalten, dass eine Firma mit Sitz in Baden-Württemberg im Rhein-Neckar-Kreis Daten über Katzenhalter_innen sammele und diese Daten an öffentliche Stellen herausgebe. Hintergrund für die Datensammlung war, dass ein baden-württembergisches Landratsamt im Zusammenhang mit einer vom Aussterben bedrohten Vogelart eine Allgemeinverfügung erlassen hat. Nach dieser ist in einem bestimmten Bereich der Gemarkung einer Stadt innerhalb eines bestimmten Zeitraumes der Freigang von Katzen grundsätzlich durch die Halter_innen zu unterbinden, da die Katzen einen bedeutenden Gefährdungsfaktor insbesondere auch für die noch flugunfähigen Jungvögel der vom Aussterben bedrohten Vogelart darstellen. Für den Fall der Zuwiderhandlung wurde ein Zwangsgeld angedroht.

Die Stadt ihrerseits hat sodann mit dem Monitoring der Vogelpopulation einen privaten Dienstleister beauftragt, damit sich der Erhaltungszustand der Population nicht verringert. Teil der Nestschutzmaßnahmen durch den privaten Dienstleister waren dabei das Monitoring und die Kontrolle von Prädatoren wie Rabenvögel und Freigängerkatzen. Im Rahmen des Monitorings wurden durch die Firma auch personenbezogene Daten von Katzenbesitzer_innen verarbeitet und sowohl an die Stadt als auch an das Landratsamt weitergegeben.

Als zuständige Datenschutzaufsichtsbehörde haben wir insbesondere geprüft, wer der für die Verarbeitung personenbezogener Katzenhalterdaten Verantwortliche im Sinne der DS-GVO ist und ob für die entsprechende Verarbeitung eine einschlägige Rechtsgrundlage vorliegt.

Bild: kwasibanane

Was haben Katzen mit Datenschutz zu tun? Nichts. Aber Katzenhalter_innen und Behörden, die die Daten von ihnen haben wollen.

Ein zentraler Grundsatz der DS-GVO ist es, dass die datenschutzrechtlichen Verantwortlichkeiten bei der Verarbeitung personenbezogener Daten klar bestimmt sein müssen. Der Erwägungsgrund 79 stellt hierbei ausdrücklich klar, dass es zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter einer klaren Zuteilung der Verantwortlichkeiten bedarf. Insoweit trägt der Verantwortliche nach Artikel 24 Abs. 1, Artikel 25 Abs. 1, Artikel 5 Abs. 2 DS-GVO die Verantwortung und Rechenschaft dafür, dass die Vorgaben der DS-GVO eingehalten und die Betroffenenrechte hinreichend gewährleistet werden. Gleichzeitig ist der Verantwortliche bei Missachtung eben dieser Vorgaben Adressat aufsichtsrechtlicher Maßnahmen. Gerade bei der Zusammenarbeit mehrerer unterschiedlicher Stellen muss im Zusammenhang mit der Verarbeitung von personenbezogenen Daten sichergestellt und jederzeit für alle Mitwirkenden erkennbar sein, wer für die konkrete Datenverarbeitung verantwortlich ist und wer als Auftragsverarbeiter lediglich eine weisungsgebundene Hilfsfunktion wahrnimmt.

In der Praxis kann die Zuordnung der Verantwortlichkeiten allerdings mitunter Schwierigkeiten bereiten, insbesondere dann, wenn sich mehrere Akteur_innen mit unterschiedlichen Beiträgen an der Datenverarbeitung beteiligen. Dann muss geklärt werden, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet, mithin Verantwortlicher nach Artikel 4 Nummer 7 DS-GVO ist. Zur Klärung dieser Frage haben wir Stellungnahmen verschiedener Stellen eingeholt. Nach Abschluss unserer Ermittlungen und Berücksichtigung der eingeholten Stellungnahmen sind wir davon ausgegangen, dass die Verantwortlichkeit bei dem Landratsamt und der Stadt lag. Der private Dienstleiter nahm auf Grundlage der Sachverhaltsdarstellungen mit dem Monitoring hingegen nur eine datenschutzrechtliche Hilfsfunktion wahr und wurde daher als Auftragsverarbeiter eingestuft. Insoweit bedurfte es zwischen dem Verantwortlichen und dem Auftragsverarbeiter eines Auftragsverarbeitungsvertrages nach Artikel 28 Abs. 3 Satz 1 DS-GVO, welcher im konkreten Fall allerdings nicht vorgelegt werden konnte. In Fällen einer zulässigen Übertragung von hoheitlichen Aufgaben an einen privaten Dienstleister muss nämlich, da über die Zwecke und Mittel

der Datenverarbeitung nicht der private Dienstleister, sondern die jeweilige öffentliche Stelle selbst entscheidet, durch jede verantwortliche Stelle ein schriftlicher Auftragsverarbeitungsvertrag mit dem privaten Dienstleister geschlossen werden.

☛ Auftragsverarbeitung Art. 28 DS-GVO

LfDI Broschüre zu Datenschutz bei Gemeinden, Kommunen ab S. 36:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/11/Brosch%C3%BCre-Gemeinden-November-2019.pdf

private Stellen:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/06/Auftragsdatenverarbeitung-DS-GVO.pdf

Muster Auftragsverarbeitungsvertrag:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/12/200429_AVV-Muster_DE_neu.pdf

In Konstellationen mit unterschiedlichen verantwortlichen Stellen, gerade auch im Zusammenwirken von öffentlichen Stellen und privaten Dienstleistern, muss neben der Prüfung, ob eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten vorhanden ist und die hoheitliche Aufgabe überhaupt an einen privaten Dienstleister übertragen werden kann, immer zwingend vor der Datenverarbeitung geprüft werden, ob Auftragsverarbeitungsverträge geschlossen werden müssen, was in solchen Konstellationen regelmäßig der Fall ist. Es ist Aufgabe des Verantwortlichen eben dies sicherzustellen und hinreichend zu dokumentieren. Wir haben alle beteiligten Stellen hierauf hingewiesen und erwarten, dass entsprechende Maßnahmen zukünftig ergriffen werden.

Privatspäre auf Social Media

Folgender Fall bezieht sich auf eine Entscheidung im Dezember 2022 (nach Drucklegung des letzten TB und daher im aktuellen Berichtszeitraum). Es ging um folgenden Sachverhalt: Wir haben eine Verwarnung gegen den Kreisverband Göppingen der Alternative für Deutschland ausgesprochen. Der Kreisverband hatte auf seiner Facebook-Seite das Foto des Baugrundstücks und künftigen Wohnortes einer Landtagsabgeordneten einer anderen Partei unter Nennung ihres Namens sowie des Bauträgers veröffentlicht. Die Landtagsabgeordnete war zuvor mit ihrer Nachbarin wegen eines Tretrollers in Streit geraten, was im Juni 2021 sogar zu einem Polizeieinsatz führte und medial als „Roller-Gate“ bezeichnet wurde.

Während der politische Streit um die sogenannte „Roller-Gate“-Auseinandersetzung und auch die entsprechende Nennung im Facebook-Beitrag als Teil – durchaus intensiver – politischer Konfrontation und damit als Teil der Meinungsfreiheit und politischen Willensbildung datenschutzrechtlich nicht zu beanstanden und auch nicht Gegenstand des Verfahrens waren, kann dies für die im weiteren Beitrag vorgenommene bewusste Verknüpfung von Namensnennung der Betroffenen, Nennung des Bauträgers und Veröffentlichung des Fotos vom Bauplatz und künftigen Wohnort der Betroffenen gerade nicht gelten. Hierfür fehlte es dementsprechend bereits an einem berechtigten Interesse und damit einer Rechtsgrundlage für die Veröffentlichung.

Es gehört zur unumstößlichen Privatsphäre der Betroffenen – auch als Abgeordnete –, mit wem diese künftig ein Haus bauen und wo sie wohnen wird. Dies gilt erst recht mit Blick auf die hiermit verbundene naheliegende Gefährdung der Betroffenen, an ihrem zukünftigen Wohnort von politischen Gegnern aufgesucht und an ihrem privaten Rückzugsort konfrontiert zu werden – bzw. die Befürchtung der Betroffenen, dass dies geschehen könnte.

In diesem Fall war es geboten, eine Verwarnung auszusprechen. Zwar ist in der (partei-)politischen Auseinandersetzung mit Blick auf die Meinungsfreiheit sowie den grundrechtlich geschützten Status von Parteien besondere Zurückhaltung bei der Verhängung von Sanktionen geboten. Hier erfolgte die Veröffentlichung privater Informationen aber ohne Zusammenhang zur politischen Auseinandersetzung, zudem sind die erheblichen nega-

tiven Folgen für die Betroffenen von Doxing (dem unerlaubten Veröffentlichen von privaten Daten wie Adresse, Telefonnummer und Arbeitgeber) zu berücksichtigen. Weil die Preisgabe der Privatsphäre über den zulässigen Raum der politischen Auseinandersetzung hinausgegangen war, war eine Verwarnung – als milderes Mittel zu einer Geldbuße – auszusprechen. Der Kreisverband, der den Post schon kurz nach Veröffentlichung gelöscht hatte, zeigte sich sensibilisiert für den zukünftigen Umgang mit personenbezogenen Daten.

Datenschutzwidrige Rechtsverteidigung? Übermittlung von Kundendaten an Rechtsanwälte und Gerichte zwecks Prozessführung

Immer wieder erreichen uns Beschwerden von Parteien eines Zivilprozesses, die der Ansicht sind, der Prozessvortrag der beklagten Gegenseite verstoße gegen den Datenschutz. Dieser Vorwurf ist nur in absoluten Ausnahmefällen begründet.

Ein Bürger verklagte seine Bank vor dem Zivilgericht auf Schadensersatz in Form von entgangenem Gewinn wegen fehlerhafter Anlageberatung. Dabei machte der Kunde geltend, die empfohlene Geldanlage sei für ihn mangels hinreichender verfügbarer Eigenmittel ungeeignet gewesen. Um dies zu widerlegen, trug die Bank Einzelheiten zu den finanziellen Verhältnissen des klagenden Kunden vor und legte dar, warum gerade angesichts dieser die befürwortete Investition für den Kunden durchaus vorteilhaft gewesen wäre. Der klagende Kunde betrachtete dies als Datenschutzverstoß und fühlte sich in seinen Rechten verletzt. In seiner Beschwerde vertrat er die Ansicht, die Bank hätte dem Gericht die ihn betreffenden Finanzdaten gar nicht erst mitteilen dürfen.

Das Verhalten der Bank war auf der Grundlage einer Interessenabwägung nach Artikel 6 Abs. 1 Buchst. f DS-GVO aus datenschutzrechtlicher Sicht nicht zu beanstanden. Verklagt ein Kunde seine Bank, so hat diese ein berechtigtes Interesse daran, sich im Zivilprozess zu verteidigen. Zu diesem Zweck darf das beklagte Kreditinstitut dem Gericht grundsätzlich diejenigen Daten übermitteln, die es zur Verteidigung für erforderlich halten darf. Dies gilt erst recht für die Übermittlung an den von der Beklagtenseite bevollmächtigten Rechtsanwalt, zumal dieser gem. § 203 Abs. 1 Nr. 3 des Strafgesetzbuchs der anwaltlichen Schweigepflicht unterliegt.

Einem berechtigten Interesse an der Datenweitergabe steht es jedoch auf Grund des Erforderlichkeitsprinzips entgegen, wenn der auf den übermittelten Daten basierende Vortrag sachfremd ist und daher von Vornherein unter keinem denkbaren Gesichtspunkt geeignet sein kann, den Klaganspruch zu entkräften. Beschränkt sich die Bank also nicht auf die Darstellung der der Anlageberatung zugrundeliegenden finanziellen Rücklagen der Klägerseite, sondern versucht sie, diese z. B. durch Offenlegung ihrer Vereinsmitgliedschaften oder ihres Konsumverhaltens allgemein zu diskreditieren, so dürfte dieser Vortrag sachfremd und nicht durch das Vorliegen eines berechtigten Interesses gedeckt sein.

Wenn das beklagte Unternehmen hiernach die Datenübermittlung zur Prozessführung für erforderlich halten darf, so kommt für die klagende Kundschaft ein entgegenstehendes Interesse an der Geheimhaltung ihrer personenbezogenen Daten regelmäßig nicht in Betracht. Zwar kann der Umstand, dass die Gerichtsverhandlung nach § 169 des Gerichtsverfassungsgesetzes (GVG) grundsätzlich öffentlich ist, für die Klägerseite eine Beeinträchtigung bedeuten. Das Gericht kann aber unter den Voraussetzungen des § 172 GVG in Fällen besonderer Schutzbedürftigkeit die Öffentlichkeit von der Verhandlung ausschließen.

Schließlich ist zu berücksichtigen, dass den Parteien im Zivilprozess aus Gründen des effektiven Rechtsschutzes sowie der Gewährung rechtlichen Gehörs ein weitgehendes Äußerungsprivileg zukommt. Daher stehen den Parteien Rechtsbehelfe gegen prozessualen Sachvortrag außerhalb des eigentlichen Rechtsstreits mangels Rechtsschutzbedürfnisses in der Regel nicht zur Verfügung. Vielmehr kommen im Gerichtsverfahren bei behaupteten Datenschutzverstößen der Gegenseite regelmäßig

prozessuale Verwertungsverbote in Betracht. Die Parteien des Rechtsstreits haben diese primär im Ausgangsprozess selbst geltend zu machen.

Festzuhalten bleibt, dass der Datenschutz den Parteien nicht die Möglichkeit nehmen soll, ihre Rechte im Zivilprozess effektiv zu verteidigen. Die Wahrung des Datenschutzes im Verfahren obliegt dabei dem Gericht.

Rasterfahndung beim VfB? Vorprüfung entkräftet Vorwürfe

Uns erreichte ein Hinweis über eine mögliche missbräuchliche Verwendung von Mitgliederdaten durch den VfB Stuttgart 1893 e.V.. Konkret stand der Verdacht im Raum, dass aus einem Abgleich von Informationen aus sozialen Netzwerken und der Mitgliederdatenbank die Identitäten von Kritikern ermittelt wurden, welche sich in sozialen Medien unter Verwendung von Pseudonymen gegen die Vereinsführung oder einzelne Personen positioniert hatten, um mit diesen außerhalb der sozialen Netzwerke in Kontakt zu treten. Auf Grund dieses Verdachts haben wir eine Vorprüfung durchgeführt, um über die Einleitung eines aufsichtsbehördlichen Verfahrens entscheiden zu können.

Im Rahmen der Vorprüfung wurden verschiedene Personen befragt sowie letztlich auch der VfB Stuttgart 1893 e.V. zu dem Vorwurf angehört. Der ursprüngliche Verdacht wurde hierdurch entkräftet. So konnte lediglich ein Fall ermittelt werden, bei dem es zu einem solchen Abgleich gekommen war. Wegen der besonderen Umstände dieses Einzelfalls – so überschritten nach unserer Einschätzung mehrere Twitter-Posts der betroffenen Person die Schwelle zur strafbewehrten Beleidung – war hier ein entsprechender Abgleich gerechtfertigt.

Ob der Datenabgleich auf Artikel 6 Abs. 1 Buchst. b DS-GVO gestützt werden konnte, bedurfte nicht der Entscheidung, da er jedenfalls nach Artikel 6 Abs. 1 Buchst. f DS-GVO legitimiert war. Der Abgleich erfolgte zur Verfolgung berechtigter Interessen des Vereins bzw. Dritter. Denn auf Grund der dokumentierten Äußerungen der von dem Abgleich betroffenen Person bestand – auch zum Schutz der Adressaten dieser Äußerungen – ein berechtigtes Interesse, mit der Person in Kontakt zu treten, um auf ein gemäßigtes Auftreten hinzuwirken. Etwaige entgegenstehende Interessen der betroffenen Person, die sich auf Grundlage des festgestellten Sachverhalts darauf beschränkten, dass die Vereinsmitgliedschaft sowie die Adressdaten nicht zur Kontaktaufnahme zwecks Gesprächsvereinbarung ermittelt und benutzt wurden, überwogen zudem nicht die berechtigten Interessen des Vereins bzw. der Vereinsmitarbeitenden, -mitglieder und -funktionäre. Auch war auf Grund des wohl nicht häufig vorkommenden Namens der betroffenen Person nicht zu befürchten, dass eine dritte, unbeteiligte Person zu Unrecht für den Inhaber des Twitter-Accounts gehalten und angeschrieben werden würde. Die Ermittlung der Anschrift zwecks persönlicher Kontaktaufnahme oder gegebenenfalls auch Abmahnung war auch erforderlich zur Durchsetzung der berechtigten Ansprüche des Vereins bzw. der von den herabsetzenden bzw. beleidigenden Äußerungen des Account-Inhabers betroffenen Vereinsmitarbeitenden, -mitglieder und -funktionäre.

Zudem konnte die entsprechende Datenverarbeitung als zweckkompatibel gemäß Artikel 6 Abs. 4 DS-GVO angesehen werden. Nach § 24 Abs. 1 BDSG können personenbezogene Daten zweckändernd auch zur Verfolgung von Straftaten und zivilrechtlicher Ansprüche verarbeitet werden. Da nach summarischer Prüfung der Anwendungsbereich des § 24 BDSG vorliegend eröffnet war, insbesondere auch dem Verein selbst neben satzungsrechtlichen Sanktionen auch zivilrechtliche Unterlassungsansprüche zustehen konnten (vgl. OLG Frankfurt, Urteil vom 21.01.2016, Az. 16 U 87/15), war als Minus hierzu eine Datenverarbeitung zur Kontaktaufnahme zwecks zukünftiger Vermeidung vergleichbarer Äußerungen ebenfalls zulässig, da weniger eingreifend für die betroffene Person. Im Übrigen wäre auch ohne Berücksichtigung des in § 24 BDSG in Umsetzung der Öffnungsklausel aus Artikel 6 Abs. 4 DS-GVO in zulässiger Weise präzisierten Rechts bei Anwendung der in Artikel 6 Abs. 4 DS-GVO genannten Abwägungskriterien zu berücksichtigen, dass der VfB Stuttgart 1893 e.V. in seinen Datenschutzinformationen darauf hinweist,

dass Zweck der Verarbeitung der Mitgliedsdaten u. a. die „Durchführung" der Mitgliedschaft sei und hier beispielhaft aufgeführt wird, dass dazu auch die „Durchsetzung von nach der Satzung möglichen Sanktionen" diene. Auch mit Blick darauf kann davon ausgegangen werden, dass der Abgleich der Mitgliederdatei mit den Daten des Twitter-Account-Inhabers nicht unvereinbar mit dem Zweck der Erhebung der Mitgliedsdaten war.

Nichts Anderes gilt für die Nutzung der so ermittelten Kontaktdaten zwecks eines Versuchs, auf den Twitter-Account-Inhaber mäßigend einzuwirken oder gegebenenfalls gegen diesen auch rechtliche Schritte einzuleiten. Diese Nutzung der Kontaktdaten war nach unserer Auffassung schon nach Artikel 6 Abs. 1 Buchst. b DS-GVO gerechtfertigt, weil sie zur Geltendmachung von Ansprüchen aus dem Sonderrechtsverhältnis zwischen Mitglied und Verein erforderlich war. Jedenfalls war sie zur Verfolgung berechtigter Interessen erforderlich, ohne dass überwiegende entgegenstehende Interessen des Account-Inhabers erkennbar wären und ohne dass diese Nutzung der zur Durchführung des Mitgliedschaftsverhältnisses erhobenen Daten im Sinne von Artikel 6 Abs. 4 DS-GVO mit dem Erhebungszweck unvereinbar wäre.

Da die Vorprüfung somit keine hinreichenden Anhaltspunkte für einen Datenschutzverstoß durch den VfB Stuttgart 1893 e.V. ergeben hatte, war von der Einleitung eines aufsichtsbehördlichen Verfahrens abzusehen.

Vereine und die Auskunftserteilung

Auskunftsersuche nach Art. 15 DS-GVO sind auch weiterhin ein wichtiger Bestandteil der Betroffenenrechte, deren Überprüfung bei unserer Aufsichtsbehörde veranlasst werden. Gerne werden diese Rechte in Anspruch genommen nach Beendigung der Vereinsmitgliedschaft. Unabhängig vom jeweiligen Anlass ist das Auskunftsrecht nach Art. 15 DS-GVO außerhalb einer missbräuchlichen Geltendmachung, deren Annahme durch EuGH und BGH enge Grenzen gesetzt wurden, immer und für alle Betroffenen durch die Verantwortlichen im Verein – auch bei wiederholter Auskunftsanfrage – zu gewährleisten. Die Schaffung einer Infrastruktur zur rechtskonformen Auskunftserteilung für Betroffene nach Art. 15 DS-GVO ist daher für jeden Verein eine Pflichtaufgabe. Wir bieten speziell für Vereine regelmäßig Schulungen zum Datenschutz an und liefern dabei Grundlagenwissen und Tipps für die Praxis.

Koppelungsverbot auch bei Vereinen relevant

Auch bei Vereinen spielt das Koppelungsverbot des Artikel 7 Abs. 4 DS-GVO eine Rolle. Gleich zwei Mal mussten wir Einwilligungen darauf untersuchen, ob diese in unzulässiger Weise in Zusammenhang mit einer anderen Dienstleistung eingeholt wurden. Das eine Mal kam es zu einer Beschwerde gegen einen Verein, welcher ein Gewinnspiel durchgeführt und die Teilnahme an dem Gewinnspiel von der Anmeldung zum Newsletter abhängig gemacht hatte. Das andere Mal fragte ein Verein bei uns an, ob er die Teilnahme an Jugendlagern von der Mitteilung von Krankheiten und einzunehmenden Medikamente machen könne, was datenschutzrechtlich einer Einwilligung (der erziehungsberechtigten Personen) bedurfte.

Der hier relevante Artikel 7 Abs. 4 DS-GVO spricht kein absolutes Koppelungsverbot aus, vielmehr muss der Koppelungssituation „in größtmöglichem Umstand Rechnung getragen werden". Das ermöglicht eine differenzierte, wertende Betrachtung, in die sämtliche Umstände einfließen müssen, die geeignet sein können, die Entschließungsfreiheit der betroffenen Person zu beeinträchtigen. Hierbei können insbesondere Faktoren wie Ungleichgewicht, Marktmacht oder Interessen der Betroffenen in die Bewertung einfließen. Weiter ist zu prüfen, ob die Dienstleistung auch ohne die Datenverarbeitung erfolgen kann („erforderlich"). Und auch die Transparenz hinsichtlich der Verknüpfung von Einwilligung und Gegenleistung ist zu berücksichtigen.

Unter Berücksichtigung aller dieser Gesichtspunkte kamen wir in beiden Fällen zu dem Ergebnis, dass

Das hilfreiche Online-Tool für Vereine und kleinere Betriebe gibt es auf der Website des beim LfDI: lfdi-bw.de/clever

die jeweiligen Einwilligungen freiwillig erfolgten und keine unzulässige Koppelung vorlag. So war im Fall der Durchführung eines Zeltlagers – wenn die Datenerhebung mit Blick auf die mögliche Haftungssituation der Betreuer schon nicht als erforderlich anzusehen war – in jedem Fall aber nach wertender Betrachtung die Einwilligung als freiwillig anzusehen, insbesondere da diese auch im Interesse der betroffenen Personen ist. Und im Fall der Aktion „Gewinnspiel gegen Newsletter" stellten wir nach Prüfung fest, dass die Teilnahmebedingungen so transparent waren, dass eine freiwillige Einwilligung in den Empfang des Newsletters anzunehmen war.

☛ Artikel 7 Abs. 4 DS-GVO

ist eine wichtige Regelung bei der Beurteilung der Freiwilligkeit einer Einwilligung und lautet wie folgt:

„Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind."

Datenschutz bei der Herausgabe von Mitgliederlisten

Im Berichtszeitraum wurden wir von einem Verein mit über 60.000 stimmberechtigten Mitgliedern frühzeitig zu Rate gezogen. So war es zu einem Mitgliederbegehren zwecks Einberufung einer außerordentlichen Mitgliederversammlung gekommen. Hierbei forderten die Antragsteller die Herausgabe einer Liste aller Mitglieder nebst Kontaktdaten, um bei diesen für ihr Begehr werben zu können. Der Verein zog uns hinzu, um eine datenschutzrechtlich einwandfreie Handhabung zu gewährleisten.

Im Rahmen unserer Beratung kamen wir hinsichtlich der einzelnen aufgeworfenen Fragen zu folgender Bewertung:

1. Rechtsgrundlage für Herausgabe einer Mitgliederliste

Es ist ständige (höchstrichterliche) Rechtsprechung, dass die Initiatoren einer außerordentlichen Mitgliederversammlung zur praktischen Durchsetzung des Einberufungsverlangens einen Anspruch gegen den Verein haben, die Anschriften der übrigen Mitglieder zu diesem Zweck zu erhalten. Zwar gibt es vereinzelte Diskussionen hinsichtlich des Prozederes und der Voraussetzungen. Unstreitig ist aber ein gegebenenfalls notwendiges berechtigtes Interesse bei der Geltendmachung von Mitgliedschaftsrechten nach § 37 BGB gegeben, weshalb dem Grunde nach der Anspruch besteht.

Nach unserer Auffassung ist die Rechtsgrundlage für eine solche Datenübermittlung (zumindest beim verfolgten Zweck der Einberufung einer außerordentlichen Mitgliederversammlung) in Artikel 6 Abs.1 Satz 1 Buchst. b DS-GVO i. V. m. § 37 BGB bzw. der Vereinssatzung zu sehen. Artikel 6 Abs. 1 Satz 1 Buchst. b DS-GVO spricht zwar von „Vertrag“, erfasst gleichwohl jedenfalls alle rechtsgeschäftlichen oder auch rechtsgeschäftsähnlichen Schuldverhältnisse.

Hierbei ist zunächst zu sehen, dass das Recht zur Einberufung einer außerordentlichen Mitgliederversammlung ein mitgliedschaftliches Recht ist, welches aus der (schuldrechtlichen) Beziehung der Vereinsmitglieder untereinander folgt. Dies kommt besonders deutlich in der (analogen) Rechtsprechung zu Mitgliedschaftsrechten in Gesellschaften hervor, wonach hier ein "Schuldverhältnis" besteht, mit dem die Mitglieder sich zur Verwirklichung und Förderung eines gemeinsamen Zwecks zusammenschließen. Auch in der ersten zum Einsichtsrecht von Vereinsmitgliedern ergangenen Entscheidung des OLG München ist von einem „vertragsähnlichen Vertrauensverhältnis“ die Rede (OLG München, Schlussurteil vom 15. November 1990 – 19 U 3483/90).

Unter Geltung des früheren BDSG ist die datenschutzrechtliche Frage der Rechtsgrundlage soweit ersichtlich offengelassen worden. In der einzig bekannten Entscheidung nach Inkrafttreten der DS-GVO hat das AG Hannover (Urteil vom 13. Februar 2019, Az. 435 C-10856/18) die datenschutzrechtliche Verarbeitungsbefugnis – ohne nähere Begründung – in Artikel 6 Abs. 1 Satz 1 Buchst. f DS-GVO gesehen. Dies könnte eventuell damit zusammenhängen, dass in der bisher dazu ergangenen Rechtsprechung die Frage eines „berechtigten Interesses“ an der Herausgabe einer Mitgliederliste und etwaiger entgegenstehender Interessen diskutiert wird. Dies dürfte wohl auf der ersten hierzu ergangenen Entscheidung des OLG München beruhen (Schlussurteil vom 15. November 1990 - 19 U 3483/90), welche ein berechtigtes Interesse diskutiert, dies aber nicht im daten-schutzrechtlichen Kontext, sondern in Zusammenhang mit der Auslegung von § 37 BGB (ebenso BGH, Beschl. vom 25. Oktober 2010 – II ZR 219/09, MMR 2011, 207: „berechtigtes Interesse (…) außerhalb des Anwendungsbereichs des § 37 BGB“).

Das Einsichtsrecht in die Mitgliederliste zwecks Einberufung einer außerordentlichen Mitgliederversammlung wird aber auch in der Rechtsprechung des BGH in § 37 BGB und damit in der Vereinsmitgliedschaft und dem damit zusammenhängenden vertragsähnlichen Verhältnis der Mitglieder verankert, welches eine Datenverarbeitung gem. Artikel 6 Abs. 1 Satz 1 Buchst. b DS-GVO erlaubt. So erkennt der BGH, dass „einem Vereinsmitglied kraft seines Mitgliedschaftsrechts ein Recht auf Einsicht

in die Bücher und Urkunden des Vereins zu(steht), wenn und soweit es ein berechtigtes Interesse darlegen kann, dem kein überwiegendes Geheimhaltungsinteresse des Vereins oder berechtigte Belange der Vereinsmitglieder entgegenstehen." (BGH, Beschluss vom 21. Juni 2010 - II ZR 219/09; Hervorhebung nicht im Original).

Die Herleitung des Einsichtsrechts/Herausgabeanspruchs wie auch spiegelbildlich der Übermittlungsbefugnis aus § 37 BGB ist auch nicht wegen des Vorrangs des Unionsrechts unvereinbar mit der DS-GVO, da Artikel 6 Abs.1 Satz 1 Buchst. b DS-GVO Einfallstor für nationale vertragsrechtliche Regelungen wie § 37 BGB ist. Hierdurch wird vereinfacht gesagt eine durch nationales Privatrecht vorgegebene/regulierte Datenverarbeitung europarechtskonform. Aus diesen Gründen ist im Rahmen der datenschutzrechtlichen Bewertung auch den durch die nationale Rechtsprechung zu § 37 BGB ergangenen Vorgaben hinreichend Rechnung zu tragen.

2. Umfang der herauszugebenden Daten (insbesondere E-Mail-Adressen sowie Mitgliedsnummern)

Unabhängig von der konkreten Rechtsgrundlage für die Datenübermittlung ist diese am Maßstab der Erforderlichkeit zu messen. Bei der Herausgabe von E-Mail-Adressen ist zu sehen, dass die Datenweitergabe letztlich der Vernetzung der Mitglieder und der Ausübung von Mitgliederrechten durch diese, konkret der Herbeiführung eines Quorums zur Einladung einer außerordentlichen Mitgliederversammlung, dienen soll. Abhängig von den Umständen kann dies auch die Herausgabe von E-Mailadressen rechtfertigen. So erschien im zugrunde liegenden Fall allein mit Blick auf die Anzahl der (stimmberechtigten) Mitglieder von über 60.000 die Verwendung von E-Mail-Adressen als wesentlich geeigneter als die postalische Anschrift, um den zuvor genannten Zweck zu erreichen. Eine Beschränkung auf postalische Kommunikation könnte, alleine wegen des damit verbundenen Aufwands und der Kosten, als eine unverhältnismäßige Beschränkung von Mitgliederrechten angesehen werden. Im konkreten Fall erlaubte auch die Vereinssatzung die Verwendung von E-Mailadressen zur Kommunikation zwischen Verein und Mitgliedern. Dementsprechend haben auch verschiedene Gerichte in der Vergangenheit einen Anspruch von Vereinsmitgliedern auf Herausgabe von E-Mailadressen bewilligt.

Hinsichtlich der Übermittlung von Mitgliedernummern kann sich dies ggf. anders darstellen, da nicht unmittelbar erkennbar ist, wofür diese im Rahmen der Geltendmachung von Minderheitsrechten, konkret der Initiative zur Einberufung einer außerordentlichen Mitgliederversammlung, benötigt werden. Bei entsprechenden Anträgen ist somit vor Übermittlung zu eruieren, wozu die Mitgliedsnummern in diesem Zusammenhang konkret benötigt werden.

3. Herausgabe der Mitgliederdaten elektronisch oder in Papierform

Nach höchstrichterlicher Rechtsprechung können Vereinsmitglieder auch einen Anspruch auf Übersendung der Mitgliederliste in elektronischer Form haben (so bereits BGH, NZG 2010, 1430 Rn. 4, beck-online). Gegen diesen Anspruch bestehen dem Grunde nach keine datenschutzrechtlichen Bedenken. Abhängig vom Übermittlungsweg unterscheiden sich jedoch die zu ergreifenden technischen und organisatorischen Maßnahmen nach Artikel 32 DS-GVO. So ist bei einer Übersendung via E-Mail insbesondere auf eine ausreichende Verschlüsselung zu achten (vgl. Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. Mai 2021, Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail).

4. Betroffenenrechte (insbesondere Informationspflichten und Widerspruchsrecht)

Hinsichtlich der Betroffenenrechte hängt die datenschutzrechtliche Bewertung ganz entscheidend davon ab, nach welcher Rechtsgrundlage die Daten an den Anspruchsteller übermittelt werden.

Nach hiesiger Ansicht erfolgt die Datenübermittlung nach Artikel 6 Abs. 1 Satz 1 Buchst. b DS-GVO

zur Erfüllung mitgliedschaftlicher Rechte und damit letztlich zur Durchführung des Mitgliedschaftsverhältnisses. Dieser konkrete Zweck ergibt sich einerseits aus gesetzlichen Vorgaben, hier aus § 37 BGB, andererseits aus der Vereinssatzung. Dieser Zweck sollte in der Datenschutzerklärung eines Vereins benannt werden, eine Nichtbenennung würde die damit zusammenhängende Datenverarbeitung aber nicht rechtsgrundlos machen. So handelt es sich hierbei um einen aus Gesetz und Satzung folgenden Zweck. Dieser ist vorgegeben, die Datenschutzinformation folgt diesem nur nach und kann ihn vorliegend nicht einschränken. Es wurde unsererseits auch als unschädlich angesehen, dass bei der Datenerhebung keine Information über die konkreten Empfänger oder die Kategorie von Empfängern (z. B. „andere Vereinsmitglieder") nach Artikel 13 Abs. 1 Buchst. e DS-GVO erfolgte. Hierdurch werden die betroffenen Mitglieder auch nicht rechtslos gestellt, da die Information über die Datenübermittlung nach Artikel 14 DS-GVO von der empfangenden Stelle (hier dem Anspruchsteller) vorzunehmen ist (vorbehaltlich einer Ausnahme nach Artikel 14 Abs. 5 DS-GVO, § 33 BDSG). Wir empfehlen aber allen Vereinen, die Datenschutzinformation für die Zukunft zwecks Klarstellung hinsichtlich Zweck und Empfänger entsprechend anzupassen (also dergestalt, dass bei einem Begehren nach § 37 BGB eine Übermittlung von Mitgliederdaten an andere Vereinsmitglieder erfolgen kann).

Zuguterletzt hängt die Frage der Berücksichtigung eines Widerspruchsrechts (durch den Verein) davon ab, ob die Datenübermittlung nach Artikel 6 Abs. 1 Satz 1 Buchst. b DS-GVO erfolgt (dann nicht) oder nach Artikel 6 Abs. 1 Satz 1 Buchst. f DS-GVO. Hiervon zu unterscheiden wäre die Frage eines etwaigen durch den Anspruchsteller zu berücksichtigenden Widerspruchsrechts bei Erhebung der Daten durch diesen, soweit die Erhebungs- und Verarbeitungsbefugnis aus Artikel 6 Abs. 1 Satz 1 Buchst. f DS-GVO folgen würde. Nach hiesiger Auffassung erfolgt aber auch die Erhebung auf Grundlage des Artikel 6 Abs. 1 Satz 1 Buchst. b DS-GVO, denn das Mitgliedschaftsrecht wirkt nicht nur zwischen Verein und einzelnem Mitglied, sondern auch zwischen den Mitgliedern untereinander. Bei dem Verein handelt es sich um eine Verbindung einer größeren Anzahl von Personen zur Erreichung eines gemeinsamen Zweckes. Dementsprechend begründet der BGH die Herausgabe von Mitgliederdaten auch wie folgt: „Die Vereinsmitglieder sind mit ihrem Beitritt zum Bekl., der einen bestimmten Zweck verfolgt – insoweit vergleichbar mit dem Beitritt zu einer Publikumspersonengesellschaft (vgl. hierzu BGH, NZG 2010, 61 = NJW 2010, 439 Rn. 9) – in eine gewollte Rechtsgemeinschaft zu den anderen, ihnen weitgehend unbekannten Mitgliedern des Bekl. getreten, zu denen auch die Kl. zählen." (Hinweisbeschluss vom 21. Juni 2010 - II ZR 219/09). Mit Blick hierauf dürfte als Rechtsgrundlage auch für die Erhebung durch den Anspruchsteller als Kehrseite zur Datenübermittlung durch den Verein ebenfalls Artikel 6 Abs. 1 Satz 1 Buchst. b DS-GVO in Betracht kommen, so dass auch dieser ein Widerspruchsrecht nicht zu berücksichtigen hätte.

Wir haben den Verein aber im Rahmen unserer Beratung darauf hingewiesen, dass sowohl die Auslegung von Artikel 13 Abs. 1 Buchst. e, Abs. 3 DS-GVO als auch die Bestimmung der Rechtsgrundlage für Datenübermittlung und -erhebung (mit Auswirkungen für ein etwaiges Widerspruchsrecht) mangels konkretisierender Rechtsprechung (insbesondere nach Inkrafttreten der DS-GVO) mit erheblichen Unsicherheiten behaftet sind. Wollte man dieser Unsicherheit begegnen, würde sich – sofern tatsächlich eine Datenübermittlung (an den Antragsteller oder einen von diesem beauftragten Treuhänder) vorgenommen wird – eine Vorabinformation durch den Verein mit Möglichkeit des Widerspruchs anbieten.

5. Herausgabe an Treuhänder

Wir wurden auch gefragt, ob eine Herausgabe an den Anspruchsteller selbst, einem von ihm benannten Treuhänder oder einen vom Verein zu benennenden Treuhänder zu erfolgen hat.

Mit Blick auf die Grundsätze der Erforderlichkeit sowie der Datensparsamkeit wird teilweise vertreten, dass eine Herausgabe nur an einen Treuhänder verlangt werden kann (vgl. Neuhöfer, SpuRt 2012, 115, entgegen LG Köln, Urteil vom 27. September

2011 – 27 O 142/11; OLG Hamburg, Urteil vom 27. August 2009 – 6 U 38/08, BeckRS 2009, 26425, beck-online, wobei der dahingehende Tenor sich aus einer entsprechenden Beschränkung des Klageantrags im Rahmen der Berufung ergab). Dies dürfte jedoch nicht mit der höchstrichterlichen Rechtsprechung vereinbar sein. So hat der BGH hinsichtlich einer Treuhänderlösung ausgeführt, dass hierdurch die Vereinsmitglieder „in datenschutz-rechtlicher Hinsicht nicht beschwert (sind). Denn es ist den Kl. als Mitgliedern eines Vereins grundsätzlich nicht verwehrt, auch selbst Einsicht in die Mitgliederliste zu nehmen bzw. die Übermittlung der dort enthaltenen Informationen in elektronischer Form an sich selbst zu verlangen." (BGH, Hinweisbeschluss vom 21.06.2010 - II ZR 219/09).

Jedoch kann es – abhängig von der konkreten Ausgestaltung der Treuhand –datenschutzrechtlich vorzugswürdig sein, wenn ein Treuhänder einbezogen würde. So wäre hierdurch – auch auf Grund einer berufsrechtlichen oder vertraglichen Schweigepflicht – die (theoretische) Gefahr eines Datenmissbrauchs – also einer zweckwidrigen Verwendung der Daten – erheblich minimiert. Zudem könnte sichergestellt werden, dass die Daten nach Erreichung des Zwecks auch datenschutzkonform gelöscht werden. Dies hängt aber ganz wesentlich von der Ausgestaltung der Treuhand ab, insbesondere davon, für wen der Treuhänder die Daten treuhänderisch hält, also für den Verein oder für den Anspruchsteller (oder in Form einer sogenannten Doppeltreuhand).

Die konkrete Ausgestaltung der Treuhand hätte auch erheblichen Einfluss auf die sonstigen datenschutzrechtlichen Pflichten. So würde in einer Abwicklung über einen für den Verein treuhänderisch

Bild: Jamillah Knowles

Menschen auf dem Weg ins Netz.

haltenden Dritten keine (rechtsfertigungsbedürftige) Datenübermittlung vorliegen (weder Rechtsgrundlage nach Artikel 6 DS-GVO noch Informationen nach Artikel 13, 14 DS-GVO erforderlich). Eine Datenübermittlung an einen Treuhänder, welcher die Daten treuhänderisch für den Anspruchsteller hält, würde dagegen eine Datenübermittlung an den Anspruchsteller darstellen. So bestimmt der Anspruchsteller über den Treuhandvertrag Zweck und Mittel der Datenverarbeitung und ist damit als Verantwortlicher gem. Artikel 4 Nr. 7 DS-GVO anzusehen. Der Treuhänder wäre datenschutzrechtlich insoweit wohl Auftragsverarbeiter für den Anspruchsteller nach Artikel 28 DS-GVO. Auch bei einer doppelten Treuhand, welche abhängig von der konkreten Ausgestaltung als gemeinsame Verantwortlichkeit nach Artikel 26 DS-GVO anzusehen wäre, könnte eine Datenerhebung auf Seiten des Anspruchstellers vorliegen.

Abschließend haben wir dem Verein dazu geraten, die Versendung der Informationsschreiben für den Anspruchsteller zu übernehmen, so dass keine Daten übermittelt werden mussten. Auf Grund der Versendung via E-Mail konnten die Kosten auch gering gehalten werden. Eine solche Kooperation bietet sich auch für andere Vereine an: Es lauern keine datenschutzrechtlichen Fallstricke, das Vertrauen der Mitglieder in den vertraulichen Umgang mit ihren Daten bleibt erhalten und zuguterletzt werden (unnötige) Kosten auf allen Seiten gespart.

Einblick in die Dienststelle

Das vergangene Jahr 2023 waren wir weiter mit der Begleitung der Prozesse der Einführung der eAkte und des neuen SAP Repro Programms im Bereich Finanzen befasst. Da das neue Hinweisgeberschutzgesetz am 2. Juli 2023 in Kraft trat, wurde aufgrund rechtswissenschaftlich fundierter Auseinandersetzung und kooperativ im Länderverbund diskutierter Optionen die Umsetzung mit ihren Schnittstellen zum Datenschutz betrieben. Eine interne Meldestelle haben wir Anfang Dezember geschaffen, die Kontakte hierzu finden sich etwa auf unserer Homepage. Im Zuge dessen haben wir auch, um anderen Stellen zu helfen, die eine Meldestelle einzurichten hatten, FAQ herausgegeben, die datenschutzrechtliche Aspekte in Zusammenhang mit dem Hinweisgeberschutzgesetz thematisieren. An anderer Stelle im Tätigkeitsbericht gehen wir ausführlich auf die FAQ ein.

☛ **FAQ Hinweisgeberschutzgesetz:**

www.baden-wuerttemberg.datenschutz.de/faq-hinweisgeberschutzgesetz

Nacharbeiten IT-Migration und weitere Digitalisierung

Auch wir digitalisieren uns immer weiter. Dieser Prozess ist ein andauernder. Für uns ist klar: Digitalisierung beschreibt auf der Ebene der Umsetzung einen dauerhaften Prozess, eine andauernde Aufgabe, ein permanentes Draufschauen und Anpassen. Im Laufe des Jahres haben wir alle Serveranwendungen, welche noch in der Dienststelle vor Ort betrieben und gemanagt wurden, sukzessive zur BITBW migriert. Die Umzüge der Telefonanlage mit Anrufbeantworter und des Formularservers verliefen reibungslos und ohne Ausfallzeiten. Der Server für das Registraturprogramm und die noch vorhandenen alten Fileserver hingegen konnten abgeschaltet werden.

Rollout und Weiterentwicklung der eAkte beim LfDI

Nachdem wir im Jahr 2022 die für die Einführung der eAkte BW notwendige Konzeptphase abschließen konnten, begann im Januar 2023 die dritte Phase der Rolloutvorbereitung. Im Rahmen von Jours Fixes und Workshops mit Vertreter_innen der Herstellerfirmen wurden die Konzepte nochmals geprüft, fortgeschrieben und anschließend in einen sogenannten Integrationsmandanten zum ersten Mal in eine eAkte-Anwendung überführt. Die Integrationsumgebung wurde anschließend fünf Wochen unter Einbeziehung von Keyuser_innen (Hauptansprechpartner_innen), der Registratur und der dezentralen Fachadministration getestet. Nach Abschluss des Testprogramms erfolgte Mitte Mai ein einwöchiger Registraturstopp und die Arbeit mit dem bisherigen Registraturprogramm wurde eingestellt. Die darin „eingefrorenen" Daten wurden in die eAkte BW überführt und der sogenannte Produktionsmandant aufgesetzt. Am 22. Mai 2023 erfolgte dann der Rollout der eAkte BW in der gesamten Dienststelle.

Solch große Umstellungen führen in der alltäglichen Praxis zu vielen Fragen. Unseren Kolleg_innen waren mit Rat und Tat zur Seite, unterstützen das Haus nach Kräften. Der Rollout bedeutete für alle Beteiligten eine sehr große Aufgabe, die mit viel Energie, Herzblut und Problemlösungskompetenz bewältigt wurde. Mit Unterstützung des Projektsteuerkreises sowie Geduld und Nachsicht aller Kolleg_innen bei uns, wenn es bei der Umstellung mal „gezwickt" hat, konnte das Rolloutprojekt der eAkte erfolgreich abgeschlossen werden. Um die Potenziale der eAkte weiter auszuschöpfen, vorhandene Prozesse zu digitalisieren und – wenn sinnvoll – neue Prozesse zu etablieren, haben wir Ende des Jahres eine Arbeitsgruppe eAkte ins Leben gerufen. Deren Arbeitsergebnisse werden dazu beitragen, das neue Instrument in der täglichen Arbeit der Dienststelle noch fester zu verankern und den Anwender_innen weitere Vorteile und Erleichterungen zu erschließen.

Regelmäßiger Personalaustausch

Nach dem bereits in den vergangenen Jahren ein regelmäßiger Personalaustausch mit anderen baden-württembergischen Behörden im Rahmen von Abordnungen, Hospitationen und ähnlichen Maßnahmen durchgeführt wurde, konnte dies nun auch einmal grenzüberschreitend durchgeführt werden. Für drei Wochen hospitierte eine Kollegin unserer Dienststelle bei der „Garante per la protezione dei dati personali", der italienischen Datenschutzaufsichtsbehörde. Mit den italienischen Kolleg_innen fand bereits zuvor eine intensive und regelmäßige Zusammenarbeit statt, die durch diese Hospitation weiter gestärkt wurde. Für die Bereitschaft, diese Hospitation durchzuführen, und die exzellente Betreuung sind wir unseren italienischen Kolleg_innen dankbar. Der Austausch mit den baden-württembergischen Behörden wurde ebenso weitergeführt, dieses Mal erneut mit der Hospitation eines Polizeibeamten in unserem Haus. Dankbar sind wir auch unseren Kolleg_innen, die sich im Rahmen der juristischen Ausbildung um die Betreuung von Referendar_innen und Praktikant_innen gekümmert haben.

Attraktivität als Arbeitgeberin

Ein weiterer Trend, der in den vergangenen Jahren sichtbar wurde, ist der vermehrte Wunsch von Mitarbeitenden, in Teilzeit zu arbeiten. Im Rahmen des Zwischenberichtes zum Chancengleichheitsplan ergab sich, dass mittlerweile etwas mehr als ein Drittel der Mitarbeitenden einer Teilzeitbeschäftigung nachgehen. Unter den Teilzeitbeschäftigten sind etwa drei Viertel Frauen und ein Viertel Männer. Der vermehrte Trend zu Teilzeitbeschäftigungen aus unterschiedlichen Gründen führt bei der Nachbesetzung durchaus auch zu Herausforderungen, unter anderem, da viele der Stellenanteile nur befristet frei und für Bewerber_innen dementsprechend weniger attraktiv sind. Auf die Lebensumstände der Mitarbeitenden und etwa ihren Wunsch nach mehr Flexibilität gehen wir gleichwohl sehr gerne ein. Mobiles Arbeiten ist heute selbstverständlicher Teil unseres Arbeitslebens. Alle Kolleg_innen der Dienststelle haben die Möglichkeit, auch von Zuhause zu arbeiten. Dies wurde während der Pandemie eingeführt. Wir behalten diese flexible Arbeitsform bei.

Digitale Rechnungsbearbeitung

Zum 1. Januar 2023 wurde landesweit eine neue SAP Version eingeführt. Trotz umfangreichen Schulungen mussten wir uns erst mit den Eigenheiten des Systems vertraut machen, Anleitungen erstellen sowie einige Arbeitsabläufe und Prozesse anpassen. So konnten die Vorteile des neuen SAP Systems schnell genutzt werden. Durch das neue SAP ist nun auch eine medienbruchfreie Verarbeitung der eRechnungen möglich, welche bereits seit dem 1. Januar 2022 gestellt werden müssen. Die eRechnungen werden automatisch vom SAP-System angenommen, was die Bearbeitung der Rechnungen erleichtert und beschleunigt. Durch die Einführung der eAkte ist in Kombination mit dem neuen SAP nun eine rein digitale Bearbeitung der Rechnungen möglich. Hierfür mussten wir auch in diesem Bereich Arbeitsprozesse anpassen, die Rechnungsbearbeitung erfolgt mittlerweile digital und kann auch in Zeiten der Telearbeit unabhängig vom Arbeitsort erledigt werden. Die Durchlaufzeit der Rechnungen kann dadurch beschleunigt werden. Weiterhin entfällt der Ausdruck der Rechnungsunterlagen, was Ressourcen schont.

Inhouse-Schulungen

Auch im Berichtsjahr 2023 hat die Stabsstelle für Deutsche und Europäische Zusammenarbeit regelmäßig Inhouse-Schulungen zu aktuellen Datenschutzthemen für das gesamte Kollegium angeboten. Durch das Angebot der Veranstaltungen in hybrider oder sogar reiner Präsenz-Form konnte dabei erfreulicherweise auch wieder ein direkter Austausch zwischen den Mitarbeitenden aller Abteilungen in unserer Dienststelle ermöglicht werden. Insgesamt neun Inhouse-Schulungen gaben Einblick in die aktuelle Arbeit der verschiedenen Abteilungen, beispielsweise zu den neuen Regelungen des europäischen Digital Services Act, zum Digitalen Euro, dem Einsatz von KI in Bewerbungsprozesse, oder zum kassenlosen Einkaufen.

Bild: Jamillah Knowles

Menschen und ihr Datenschatten.

Vom Schreibtisch des LfDI

Mit diesem Tätigkeitsbericht soll ein neues Format etabliert werden, in dem das vergangene (Halb-) Jahr auch aus persönlicher Perspektive der Behördenleitung Revue passiert.

Schon vor Amtsantritt am 3. Juli 2023 und noch in Eigenschaft als Hochschullehrer gab es Gelegenheit, im Rahmen des Impulses „Informationsgerechtigkeit und Transparenz" auf den 4. IFG-Days (28. und 29. Juni 2023) im Stadthaus Mannheim das engagierte Team der Abteilung Informationsfreiheit des LfDI kennenzulernen.

Die ersten Wochen der Amtsführung standen ganz im Zeichen des Kennenlernens der Dienststelle und ihrer 81 Mitarbeitenden. In zahlreichen Einzelgesprächen und Gruppenterminen ging es darum, in die Persönlichkeit der Dienststelle hineinzuhören. Ziel war auch, gemeinsam eine Vision und Agenda für die Tätigkeit der Behörde in den kommenden Jahren zu entwickeln. Über die Gespräche ließ sich die große Vielfalt individueller Kompetenzen, Interessen und unterschiedlicher Schwerpunkte des behördlichen Schaffens feststellen.

Schön zu sehen war, wie dies mit dem weiten Aufgabenkatalog korrespondiert, der in Artikel 57 Absatz 1 DS-GVO zur Überwachung und Durchsetzung des Datenschutzrechts ebenso verpflichtet, wie zur Sensibilisierung der Öffentlichkeit für Risiken im Zusammenhang mit der Verarbeitung von Daten. Die Beratung von Unternehmen und

öffentlichen Stellen bei legislativen und administrativen Maßnahmen ist nach dem DS-GVO-Pflichtenkatalog ebenso zu leisten wie einer Pflicht zum Weitblick zu entsprechen ist, innerhalb der die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken in ihrer gesamtgesellschaftlichen Dimension gewürdigt werden muss.

Dieser Aufgabenkatalog sieht keine starre Priorisierung vor, in der etwa festgelegt wäre, dass Beratung und Öffentlichkeitsarbeit im Zweifel zu Gunsten eines (wie auch immer zu umreißenden) behördlichen „Kerngeschäfts" zurückzustehen haben. Daher gilt, und das wird auch Teil der gemeinsamen Vision der Dienststelle sein müssen: Pflicht ist Kür ist Pflicht und jeder Beitrag aus der Mitarbeitendenschaft gleich wichtig.

Persönlich eindrucksvoll war schließlich auch, wie das gleich mehrfach im Aufgabenkatalog der DS-GVO adressierte Kooperationsgebot in der zwischenbehördlichen Praxis mit Leben ausgefüllt wird. Das geschieht auf nationaler Ebene über wöchentliche Videokonferenzen, die Datenschutzkonferenz und die Konferenz der Informationsfreiheitsbeauftragten, die jeweils durch Vor-, bzw. Zwischenkonferenzen ergänzt werden. Das in der öffentlichen Diskussion bisweilen bemühte Narrativ von ständig divergierenden Rechtsansichten unter den Aufsichtsbehörden kann von dieser Stelle aus mit nunmehr frisch gewonnener Innenansicht nicht bestätigt werden. Die Einheitlichkeit in der Rechtsanwendung ist gemeinsamer Anspruch. Gleichwohl kann es im Einzelfall herausfordernd sein, Unabhängigkeit zu konzertieren.

Thematisch standen die ersten sechs Monate des neuen Landesbeauftragten unter dem Eindruck der zahlreichen Neuerungen im europäischen Digital- und Datenrecht, wobei die Herausforderungen durch Künstliche Intelligenz eine Sonderrolle spielten. In diesem Kontext stand die im Bericht näher dargestellte Diskussionsrunde „Zukunft des Datenschutzes – Ist die DS-GVO bereit für KI?" ebenso wie zahlreiche Vorträge sowohl vor Fachpublikum als auch der interessierten Öffentlichkeit sowie unsere KI-Woche. Höhepunkt der umfassenden inhaltlichen Auseinandersetzung mit KI war die Herausgabe des Diskussionspapiers „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz", das wir nach intensivem innerbehördlichen Austausch veröffentlicht haben. In dieser Form war es das bundesweit erste Papier, das nunmehr auch in englischer Sprache vorliegt und so von Baden-Württemberg in die europäische Debatte eingebracht wird.

Ausblick

Vom Schreibtisch im Büro des LfDI im 4. Stock der Lautenschlagerstraße 20 hat man einen guten Blick Richtung Königstraße und damit in die pulsierende Mitte des gesellschaftlichen und wirtschaftlichen Lebens im Ländle. Wie wird sich das in den kommenden Jahren verändern und welche Rolle werden dabei Datenschutz und Informationsfreiheit spielen?

Absehbar ist, dass durch die neuen Digital- und Datenakte sowie die KI-Verordnung und die dort neu etablierten Entitäten neue Kooperations- und Abstimmungsverfahren nicht nur zwischen Datenschutzbehörden notwendig werden, was Kapazitäten binden wird. Die exponentiell steigende Geschwindigkeit technischer Innovation stellt das Recht und seine Durchsetzung vor enorme Herausforderungen. Zukunftsfähige Behörden müssen ebenso innovativ, technikversiert und interdisziplinär anschlussfähig sein.

Ein hohes Gut, nicht nur aus Sicht der vielen Unternehmen, Vereine und öffentlichen Stellen ist die Rechtssicherheit. In den nunmehr über 5 Jahren ihrer unmittelbaren Anwendbarkeit ist die DS-GVO als Kern des europäischen Datenschutzrechts durch Rechtsprechung und Praxis umfänglich konkretisiert worden. Auch wenn dieser Weg noch nicht zu Ende ist: Die DS-GVO ist fit für die Zukunft. Ihr liegt ein europäisches Werteverständnis zu Grunde, das auch das künftige Digital- und Datenrecht prägen wird.

Wir werden unseren Beratungsansatz konsequent fortführen und nach Möglichkeit ausbauen. Ein innovativer Ansatz der DS-GVO ist die Erkenntnis, dass Datenschutz so früh wie möglich mitzuden-

ken ist und bereits bei der Konzeption von Produkten und Dienstleistungen eine Rolle spielen sollte. „Privacy/Data Protection by Design“ kann sich, jedenfalls langfristig, zum internationalen Wettbewerbsvorteil entwickeln.

Das gilt vor allem auch für die Entwicklung und die Anwendung von Künstlicher Intelligenz. Dass Unternehmen durch mehr Datenschutz größere Gewinne erzielen, als sie die korrespondierenden Maßnahmen kosten, zeigt eine jüngst veröffentlichte Studie, bei der im Sommer 2023 insgesamt 2.600 Sicherheits- und Datenschutzexpert_innen aus Unternehmen in zwölf Ländern befragt wurden. Nach der selben Studie sahen zwei Drittel der Befragten Gefahren für ihre Unternehmen durch Künstliche Intelligenz und die Veröffentlichung von vertraulichen Informationen.

☛ **Privacy as an Enabler of Customer Trust:**

Cisco 2024 Data Privacy Benchmark Study:

www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf

Im kommenden Jahr soll Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 DS-GVO) einen inhaltlichen Schwerpunkt der Behörde bilden. In diesem Zusammenhang werden wir uns weiter mit „Deceptive design patterns“ befassen. Wir werden zu Artikel 25 DS-GVO Arbeitspapiere veröffentlichen, den Inhalt der Vorschrift soweit erforderlich aber auch rechtsdurchsetzend adressieren.

Statistischer Überblick

In Baden-Württemberg leben rund 11,28 Millionen Menschen (Stand 2022). Rund 480.000 Unternehmen (rechtliche Einheiten mit steuerbarem Umsatz und sozialversicherungspflichtig Beschäftigten, Stand 2019), rund 86.000 Vereine, rund 4.500 Schulen, 1.101 Städte und Gemeinden, 35 Landkreise sowie zahlreiche weitere Einrichtungen und Unternehmungen zählen wir hier. Baden-Württemberg ist ein innovatives Forschungsland, der Gesundheitssektor ist sehr wichtig, Künstliche Intelligenz ist von besonderer Bedeutung, die Start-up Kultur ausgeprägt.

Im Berichtszeitraum erreichten uns 3.817 Beschwerden (+21 im Vergleich zum Vorjahr). Dieser Wert entspricht etwa denen der Jahre kurz vor und kurz nach der Corona-Pandemie. Die Zahl der Kontrollen hat sich mehr als verdoppelt und liegt bei 71 (+38) Die Zahl der Datenpannenmeldungen lag bei 2.913 (+166). Unsere Beratungen folgen dem Trend der vergangenen Jahre. Die Zahl der konkreten Einzelfallberatungen war im vergangenen Jahr rückläufig mit 1.682 (-253), während die strukturelle Beratung durch unser Bildungszentrum BIDIB öfter in Anspruch genommen wurde und erreichte mit 3.732 Anmeldungen einen neuen Bestwert (+477). Unsere Handreichungen wurden sehr gut in Anspruch genommen. Auf unserer Homepage wurde die Seite mit unserem „Diskussionspapier Rechtsgrundlagen im Datenschutz beim Einsatz von KI“, welches wir Mitte November 2023 veröffentlicht haben, bislang über 12.000 Mal aufgerufen; unsere FAQ zum Hinweisgeberschutzgesetz, fast zeitgleich veröffentlicht, über 6.500 Mal. Unsere FAQ zu Cookies und Tracking sind ein Dauerbrenner und verzeichneten im vergangenen Jahr ebenfalls über 12.000 Aufrufe. Unser Fachgespräch zur KI-Regulierung am 13. Juli etwa wurde im Anschluss über 6.000 Mal aufgerufen. Mit 185 eingeleiteten Bußgeld liegt die Zahl um 28 unter dem Wert von 2022.

Statistische Übersicht – Zeitraum jeweils vom 1. Januar – 31. Dezember

	2016	2017	2018	2019	2020	2021	2022	2023
Beschwerden	2.048	3.058	3.902	3.757	4.782	4.708	3.796	3.817
Kontrollen	16	55	13	111	31	10	33	71
Beratungen[1]	1.515	1.786	4.440	3.842	3.285	2.206	1.935	1.682
Anmeldungen Bildungs- und Beratungszentrum BIDIB					785	2.016	3.255	3.732
Datenpannen	68	121	900	2.030	2.321	3.136	2.747	2.913
Bußgeldverfahren (eingeleitet)			138	233	174	136	213	185

1 ohne telefonische Beratung

Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Baden-Württemberg

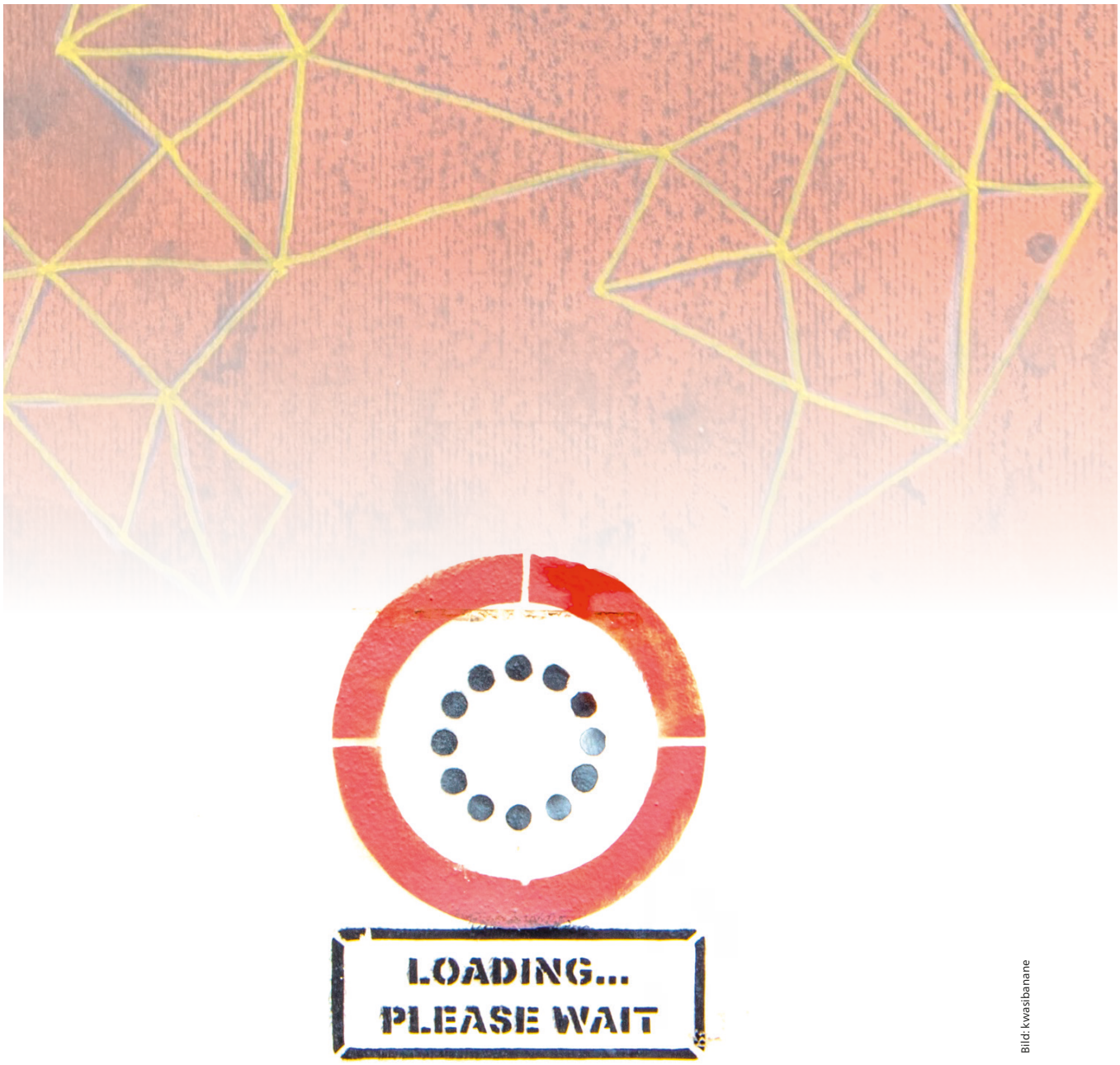


Bild: kwasibanane

Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Baden-Württemberg