Innovation mit Datenschutz.
Für Menschen.
Einfach machen.

Unsere Freiheiten:
Daten nützen – Daten schützen

Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Baden-Württemberg

40. Tätigkeitsbericht
Datenschutz 2024

Herausgegeben von
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Prof. Dr. Tobias Keber
Lautenschlagerstraße 20, 70173 Stuttgart
Telefon: 0711/615541-0
www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
Mastodon: bawü.social/@lfdi
PeerTube: tube.bawü.social
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Redaktion: Prof. Dr. Tobias Keber,
Cagdas Karakurt, Simone Markovic, Feli Stary (alle Koordinierungs- und Pressestelle)
Gestaltung, Reinzeichnung, Barrierefreiheit: kwasibanane (Reinhardt Jacoby)
Februar 2025
Veröffentlicht als Landtags-Drucksache 17/8500

Innovation mit Datenschutz.
Für Menschen.
Einfach machen.

40. Datenschutz-Tätigkeitsbericht
des Landesbeauftragten für den Datenschutz und
die Informationsfreiheit Baden-Württemberg 2024

Baden-Württemberg

Inhalt

ABSCHNITT 2

Prof. Dr. Tobias Keber

Vorwort

Vor Ihnen liegt der 40. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg. Das Jubiläum gibt Anlass, auf den ersten Bericht zurückzublicken, der im Jahr 1980 von der damaligen Beauftragten „nur" für den Datenschutz (Informationsfreiheit auf landesrechtlicher Ebene gab es noch nicht) Frau Dr. Ruth Leuze vorgelegt wurde. Bereits drei Jahre vor der Grundsatzentscheidung des Bundesverfassungsgerichts zur informationellen Selbstbestimmung (Volkszählungsurteil) war dort ebenso Progressives wie Zeitloses zu lesen:

» *Ziel des Datenschutzes ist es, in unserer hochentwickelten Informationsgesellschaft den Missbrauch persönlicher Daten zu verhindern. […] Seine Aufgabe ist, den angemessenen Ausgleich zwischen Informationsbedürfnis und Informationszwang einerseits und der Wahrung des Personseins andererseits in Staat und Gesellschaft, am Arbeitsplatz und im privaten Lebenskreis zu sichern* «
(S. 7 der LT-Drucksache 8 / 830).

Herausgefordert war der Datenschutz schon damals u. a. durch eine Praxis,

» *die abgewogene Einzelentscheidung zunehmend durch schematisierte Bescheide zu ersetzen* « und

» *Datenschutz als Vorwand für mangelnde Bereitschaft zum Verwaltungshandeln oder als Begründung nicht plausibler Verwaltungsentscheidungen zu benutzen.* « (S. 8 der LT-Drucksache 8 / 830).

Die Situation in der Privatwirtschaft konnte die Datenschutzbeauftragte damals nicht adressieren, denn dieser Bereich oblag der Aufsicht des Innenministeriums, die Zuständigkeiten wurden erst 2011 beim Landesbeauftragten zusammengeführt. Hintergrund dieser Zäsur war die Entscheidung des Europäischen Gerichtshofs vom 9. März 2010 in einem Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland, worin festgestellt wurde, dass die bisherige Aufsichtsstrukur in Deutschland europäischen Vorgaben nicht entsprach. Die organisatorisch einschneidenden Veränderungen führten letztlich auch dazu, was aufmerksame Leser_innen dieser Zeilen bereits kritisch hinterfragt haben dürften: wie man logisch stimmig vom 1. Tätigkeitsbericht 1980 zum 40. Tätigkeitsbericht für das Jahr 2024 gelangt, erschließt sich nicht auf Anhieb. Tatsächlich wiesen die Berichte zeitweise (30. TB 2010 / 2011 – 33. TB 2016 / 2017) einen zweijährigen Berichtszeitraum aus, was den neuen Strukturen und organisatorischen Zuwächsen geschuldet war. Seit der „datenschutzrechtlichen Zeitenwende" (vgl. Vorwort 34. Tätigkeitsberich

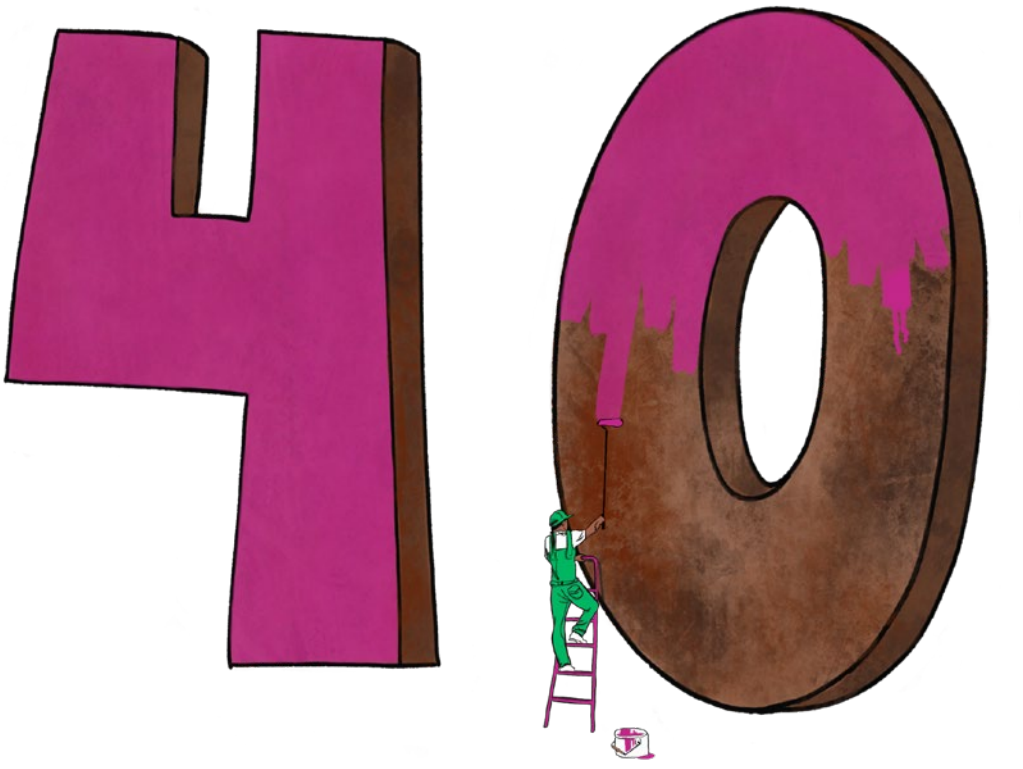
Datenschutz) 2018 gilt wieder – übrigens von der DS-GVO explizit so vorgesehen (Art. 59 Satz 1 DS-GVO) – der Jahresturnus.

Wie im letzten Tätigkeitsbericht bereits eingehend dargestellt, steht das vielschichtige Aufgabenfeld des Landesbeauftragten weiterhin unter dem besonderen Eindruck eines ebenso schnell wie ambitioniert erweiterten Europäischen Daten- und Digitalrechts. Die Vielzahl von Beratungsanfragen zum Zusammenspiel der unterschiedlichen neuen Rechtsakte und der Datenschutzgrundverordnung, die grundsätzlich unberührt bleiben soll, hat die Kapazitäten der Behörde im vergangenen Jahr über die Auslastungsgrenze hinaus beschäftigt. Entlastung ist nicht in Sicht und 2025 wird neben dem Tagesgeschäft ein weiterer Umzug der Behörde zu stemmen sein, die sich zuletzt 2011 und 2021 örtlich umorientieren musste.

Im 40. Tätigkeitsbericht finden sich neue Gestaltungselemente, die zur Verständlichkeit und Lesbarkeit des Textes beitragen sollen. Den Beiträgen ist jeweils eingangs zugeordnet, aus welchem aufsichtsbehördlichen Aufgabenbereich der DS-GVO der Sachverhalt stammt. Der weite Katalog des Artikel 57 DS-GVO mit seinen insgesamt 22 explizit formulierten Feldern wird so konkret mit Leben gefüllt. Gegliedert ist der Bericht in zwei größere Kapitel, einen ersten Abschnitt mit abteilungsübergreifenden Schwerpunkten und den großen Entwicklungslinien im Daten- und Digitalrecht sowie einen zweiten Abschnitt mit Berichten aus den Fachabteilungen.

Ihr Landesbeauftragter

Prof. Dr. Tobias Keber



Sie lesen gerade den 40. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Vom Schreibtisch des Landesdatenschutzbeauftragten

Das Jahr 2024 stand bei all seiner thematischen Vielfalt unter besonderem Einfluss der am 1. August 2024 in Kraft getretenen EU-Verordnung zur Künstlichen Intelligenz (KI-VO). Die Diskussionen rund um die Zuständigkeiten bzgl. der Aufsicht über die Einhaltung der KI-VO und die Rolle der Datenschutzbehörden dabei machten offenbar, welche Sicht die politische Landschaft zum Teil auf den Datenschutz hat. Auch wenn die Datenschutzbehörden aufgrund der bei KI-Systemen zumeist verarbeiteten personenbezogenen und -beziehbaren Daten für die sektorspezifische Zuständigkeiten nach KI-VO als Marktüberwachung naheliegen würden, war und ist der politische Diskurs davon geprägt, nicht die „gleichen Fehler wie bei der DS-GVO" machen zu wollen. Insoweit wird ein verzerrtes Bild überschießender Regulierung und Rechtsdurchsetzung gezeichnet, welches Innovation behindere.

> ☛ **Weitere Informationen**
>
> Vgl. zum Ganzen auch: Keber / Henning in EuDIR, Heft 1 / 2025

Narrative im Realitätscheck

Ein plakatives Beispiel für das angesprochene Zerrbild ist auch das Narrativ, den Datenschutz in natürlicher Verbundenheit mit Bürokratie zu sehen. So fanden sich Vorschläge zur Entbürokratisierung bei Ehrenämtern und Vereinen, die sich gegen eine „Übererfüllung der DS-GVO" aussprachen, z. B. durch die Abschaffung der Pflicht zur Bestellung eines Datenschutzbeauftragten für ehrenamtlich geführte Vereine ebenso wie die Abschaffung von Bußgeldern bei Erstverstößen. Mit Blick auf die Bußgeldrealität in Baden-Württemberg kann konstatiert werden, dass hierzulande noch nie seit Inkrafttreten der DS-GVO ein Bußgeld gegen einen ehrenamtlich geführten Verein verhängt wurde.

Datenschutz ist Bürokratie? Das könnte man tatsächlich bejahen, wenn „Bürokratie" im ursprünglichen Wortsinn gemeint ist und damit einen Zustand der Verlässlichkeit, Gleichbehandlung, Ordnung und Rechtssicherheit beschrieben wird. Es geht um Vertrauen in staatliche Strukturen. Hier knüpften wir mit einer Veranstaltung an: Im Austausch mit Vertretungen der Ministerien (genauer der Entlastungsallianz Baden-Württemberg) und der kommunalen Spitzenverbände Baden-Württemberg ebenso wie mit Vertreter_innen direkt aus kommunalen Stellen zeigte sich, dass der Datenschutz als hohes Gut für einen freiheitlich geprägten Staat eingeschätzt wird, den es zu bewahren gilt.

Infokasten

Dies deckt sich auch mit einer repräsentativen Studie zu Künstlicher Intelligenz und Kompetenz aus dem Jahr 2023, gefördert vom Bundesministerium für Familie, Senioren, Frauen und Jugend. Obgleich sich nur eine Minderheit der Befragten beim Thema Datenschutz als (eher) kompetent erlebt, hat diese Fähigkeit für die meisten (92 Prozent) eine (große) Bedeutung. 97 Prozent der Befragten messen dem Schutz der eigenen Online-Daten eine (große) Bedeutung zu. Hier wird Handlungsbedarf bei der Tech-Branche, Bildung und Politik gesehen, da Datenschutz als hochrelevantes Thema für ein souveränes Leben in der digital vernetzten Welt eingeschätzt wird. Vgl. Cousseran / Lauber / Herrmann / Brüggen, Kompass: Künstliche Intelligenz und Kompetenz 2023, S. 32, 54: zenodo.org/records/10058588

Im schlechten Fall sorgen Unwissenheit, mangelnde personelle, fachliche und zeitliche Ressourcen bei den verantwortlichen Stellen dafür, dass Datenschutz

LfDI Prof. Dr. Tobias Keber; Tabea Gernoth-Laber, LRA Neckar-Odenwald Kreis; Norbert Brugger, Dezernent Städtetag BW (v.l.n.r.).

als Hemmnis und Belastung in den Behörden wahrgenommen wird. Hier schließt sich also im Konkreten der Kreis, dass die Sensibilisierung für die Bedeutung des Datenschutzes als Ausdruck der informationellen Selbstbestimmung weiterhin durch Veranstaltungen und Publikationen über die Datenschutz-Fach-Community hinaus betrieben werden muss. Hierbei sind auch die Aufsichtsbehörden in der Pflicht, Datenschutzrecht trotz mancher Widrigkeiten selbstbewusst und lösungsorientiert zu verteidigen.

Weitere Informationen

Kommunaler Fachtag am 5. November 2024:
www.baden-wuerttemberg.datenschutz.de/diskussionsrunde-zu-grundrechten-und-entbuerokratisierung

Positionspapier Gemeindetag Baden -Württemberg Kommunaler Landesverband kreisangehöriger Städte und Gemeinden, Digitales Rathaus – Gemeinsam zur zukunftsfähigen Verwaltung September 2024, S. 6:
gemeindetag-bw.de/system/files/downloads_buch/Positionspapier-Verwaltungsdigitalisierung_final.pdf

Entlastungsallianz und ihre Agenda:
stm.baden-wuerttemberg.de/de/themen/verwaltungsmodernisierung-und-buerokratieabbau/entlastungsallianz-fuer-baden-wuerttemberg

TikTok: Meinungsbildung und der Datenschutz

Diese Notwendigkeit zeigt sich auch schon seit vielen Jahren beim Thema des Social Media-Einsatzes zur behördlichen Kommunikation mit den Bürger_innen, die 2024 durch die zunehmende Nutzung von TikTok durch staatliche Stellen erneut Fahrt aufnahm. Nicht nur Ministerien, auch Fraktionen wählen vermehrt den in der Kritik stehenden Dienst des chinesischen Konzerns Bytedance, um eine junge Zielgruppe mit behördlichen und politischen Informationen zu versorgen.

Hier veranschaulicht sich ein Dilemma, mit dem der Datenschutz in ähnlicher Weise bei abzuwägenden Rechtsgütern immer wieder zu kämpfen hat. In Zeiten von Desinformation und Manipulation ist der Bedarf groß, ein Gegengewicht zu setzen – genau dort, wo diese Kommunikation stattfindet. Dennoch stellt sich die Frage, wie weit öffentliche Stellen ihre rechtsstaatlich begründete Vorbildfunktion zu diesem Zweck suspendieren dürfen. Aus datenschutzrechtlicher Sicht ist bei der Nutzung von TikTok nämlich zu bezweifeln, ob die Verarbeitung personenbezogener Daten den Anforderungen der in Art. 5 und Art. 25 DS-GVO geregelten

Vorgaben gerecht wird, ob sie auf einer gültigen Rechtsgrundlage nach Art. 6 DS-GVO beruht und ob die spezifischen Anforderungen des Art. 8 DS-GVO an die Datenverarbeitung von Minderjährigen sowie Art. 13 und 14 DS-GVO an die transparente Information der betroffenen Personen abgebildet werden. Ähnlich wie bereits bei Twitter und Facebook suchen wir auch bei der Nutzung von TikTok den Austausch und geben Hilfestellungen, ohne dabei die zahlreichen datenschutzrechtlichen Probleme bei der Nutzung dieses Dienstes unbeachtet zu lassen. Womöglich kann der Ausgang der noch anhängigen Verfahren zum Betrieb von Facebook Fanpages durch Regierungsstellen eine (erste) Weichenstellung auch für den Einsatz von TikTok leisten. Abzuwarten bleibt auch, welchen Einfluss die voraussichtlich im Herbst 2025 zu erwartende Verordnung des Europäischen Parlaments und des Rates über die Transparenz und das Targeting politischer Werbung haben wird, die sich massiv auf die Rechtmäßigkeit der Nutzung von Diensten wie TikTok im politischen Kontext auswirken könnte.

☛ Weitere Informationen

Zur datenschutzrechtlichen und -ethischen Einordnung siehe Keber / Henning, Olaf Scholz und die auf TikTok herrschenden Datenschutzpraktiken, 13.05.2024: netzpolitik.org/2024/wahlkampf-olaf-scholz-und-die-auf-tiktok-herrschenden-datenschutzpraktiken

Checkliste des LfDI BW zum Einsatz von TikTok: www.baden-wuerttemberg.datenschutz.de/datenschutz-oeffentliche-stellen-tik-tok

Untersagung des Betriebs einer Fanpage der Bundesregierung durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 17.02.2023: www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Bescheid-Facebook-Fanpage.pdf

Untersagung der Nutzung einer Fanpage der Sächsischen Staatskanzlei durch die Sächsische Datenschutz- und Transparenzbeauftragte, 07.07.2023: datenschutz.sachsen.de/download/20230707_Bescheid_Untersagung_Facebook_SK.pdf

Künstliche Intelligenz (KI) und Datenschutz

Zurück zum eingangs erwähnten Einfluss der KI auf die datenschutzrechtliche Arbeit der Aufsichten, von denen auch mehrere gemeinsame Positionen der Datenschutzkonferenz (DSK) im Jahr 2024 Zeugnis sind.

In der Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ vom 6. Mai 2024 adressierte die DSK die Auswahl, Implementierung und Nutzung von KI-Anwendungen, gab Empfehlungen zu Zweckbestimmung, Transparenzpflichten und Betroffenenrechten und zeigte – auch anhand von Beispielen – wichtige Kriterien entlang der Vorgaben der Datenschutz-Grundverordnung auf. Auch auf der Strategieklausur vom 30. August bis 1. September 2024 war KI ein zentrales Thema. Die DSK betonte die parallele Geltung von KI-Verordnung und DS-GVO und hob ferner hervor, dass ein kohärentes europäisches Daten-, Digital- und KI-Recht einer sorgfältigen Analyse und Diskussion über passgenau spezifische datenschutzrechtliche Anforderungen bedarf, die beim Ringen um die KI-Verordnung ausgeblendet wurden. Auf der 108. DSK am 14. / 15. November 2024 wurde ein neuer Arbeitskreis Künstliche Intelligenz eingerichtet, dem es künftig obliegen wird, die Entwicklung der KI-Technologie und ihrer Regulierung zu beobachten, Handlungsempfehlungen zu geben und die innovationsfreundliche und risikospezifische Aufsichtspraxis zu fördern. Den Vorsitz des Arbeitskreises, in dem die technische und rechtliche Expertise der Datenschutzbehörden des Bundes und der Länder vereint sind, haben Rheinland-Pfalz und Baden-Württemberg.

© Illustration: Y. Dwiputri

Orientierungshilfen-Navig

Fundstellenübersicht zu zehn zentralen Vorgaben des Datenschut
Stand Juli 2024.

	A. EDPS Guidelines on generative AI and the EUDPR (2024, PDF)↗ *Datenverarbeitung durch EU-Organe*	B. Report der EDSA Taskforce ChatGPT (2024, PDF)↗	C. DSK: Orientierungshilfe zu KI und Datenschutz (2024, PDF)↗	D. LfDI BW: Rechtsgrundlagen zum Einsatz von KI (2023)
1. Grundsatz der Datenrichtigkeit Art. 5↗ I lit. d) DSGVO	**(+)** S. 15 f. (Art. 4 I lit. d) VO 2018/1725)	**(+)** Rn. 29 ff. sowie im Fragebogen im Annex, S. 11	**(+/–)** Recht auf Berichtigung Rn. 27, Überprüfung der Richtigkeit der Ergebnisse Rn. 64 f.	**(–)**
2. Grundsatz der Datenminimierung Art. 5↗ I lit. c) DSGVO **Zweckbindungsgrundsatz** Art. 5↗ I lit. b) DSGVO	**(+)** Datenminimierung: S. 14 (Art. 4 I lit. c) VO 2018/1725) **(+/–)** Zweckbindung: nur sehr indirekt („consistent with original purpose"), S. 12	**(+/–)** nur im Rahmen des Fragebogens im Annex, S. 10	**(+)** Zweckbindung Rn. 1 f.	**(+/–)** Berücksichtigung Datenminimierung bei Art. 6 I lit. f DSGVO (S. 17) u. § 13 LDSG BW (S. 25) **(+)** Zweckänderung S. 15
3. Personenbezug Art. 4↗ Nr. 1 DSGVO	**(+)** S. 7 (Art. 3 Nr. 1 VO 2018/1725)	**(–)**	**(+)** Rn. 4 ff., 7 f., 48 ff.	**(+)** insbes. S. 6
4. Rechtsgrundlagen für die Datenverarbeitung Art. 6↗ I u. 9↗ II DSGVO	**(+)** S. 11 ff. (Art. 5 und 10 II VO 2018/1725)	**(+)** Rn. 13 ff., ebenso im Fragebogen S. 12 f.	**(+)** Rn. 9 ff. (zudem Verweis auf Positionspapier LfDI BW), Rn. 62 (im Zusammenhang mit sensiblen Daten)	**(+)** insbes. S. 11 ff.
5. (Mit–)Verantwortlichkeit Art. 26↗ (und 28↗) DSGVO	**(+)** S. 6	**(+/–)** Rn. 23 ff. in Zusammenhang mit Fairness-Prinzip, „Abwälzung" der Verantwortlichkeit auf betroffene Personen; im Rahmen des Fragebogens S. 14	**(+)** Rn. 32 ff.	**(+)** S. 9 ff.
6. Transparenzgebot und Informationspflichten Art. 5↗ I lit. a und 12 ff. DSGVO	**(+)** S. 17 (Art. 14 VO 2018/1725)	**(+)** Rn. 27 f., ebenso im Fragebogen S. 13	**(+)** Rn. 21 ff.	**(+)** S. 12 (im Zusammenhang mit informierter Einwilligung)
7. Auskunftsanspruch Art. 15↗ DSGVO **Recht auf Löschung** Art. 17↗ DSGVO	**(+/–)** allgemein Betroffenenrechte S. 22	**(+)** allgemein Betroffenenrechte Rn. 32 ff.	**(+)** nur Recht auf Löschung Rn. 26, 28 f.; „weitere Betroffenenechte" Rn. 30	**(+)** nur Recht auf Löschung S. 12
8. Automatisierte Entscheidungen und Profiling Art. 22↗ DSGVO	**(+)** S. 18 (Art. 24 VO 2018/1725)	**(–)**	**(+)** Rn. 12 ff.	**(–)**
9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen Art. 25↗ DSGVO	**(+)** S. 9 (Art. 27 VO 2018/1725)	**(+)** Rn. 7 knappe Bezugnahme; Rn. 35 im Zusammenhang mit Betroffenenrechten	**(+)** Rn. 43	**(+/–)** S. 7 (Bewertung Personenbezug), S. 18 Fn. 57 (Berücksichtigung bei Art. 6 I lit. f DSGVO)
10. Datenschutz-Folgenabschätzung Art. 35↗ DSGVO	**(+)** S. 9 f. (Art. 39 u. 89 VO 2018/1725)	**(+/–)** nur im Rahmen des Fragebogens im Annex, S. 11	**(+)** Rn. 38 ff.	**(–)**

Der Orienteriungshilfen-Navigator ONKIDA des LfDI BW steht auf seiner Homepage:
www.baden-wuerttemberg.datenschutz.de/onkida/ONKIDA.pdf

ator KI & Datenschutz (ONKIDA)

zrechts in aufsichtsbehördlichen Orientierungshilfen zu „Künstlicher Intelligenz“.

Einstiegsvideo (PeerTube)

E. BayLDA: Checkliste Datenschutz-konforme KI (2024, PDF)↗	F. Hamburger BfDI: Checkliste zum Einsatz LLM-basierter Chatbots (2023, PDF)↗	G. CNIL: Recommendations on the development of AI systems („How-to sheets“) (2024)↗	H. DSB Österreich: FAQ KI und Datenschutz (2024)↗	I. DSK: Positionspapier zu TOM bei Entwicklung und Betrieb von KI-Systemen (2019, PDF)↗	J. DSK: Hambacher Erklärung zur KI (2019, PDF)↗
(+/–) Recht auf Berichtigung, S. 6, 10	(+/–) Überprüfung der Richtigkeit des Ergebnisses S. 4	(+/–) „data cleaning“, „monitoring and updating“ Sheet 7	(+)	(–)	(–)
(+/–) Zweckbindung nur eher indirekt S. 6, 8, 11 (Checkliste)	(–)	(+) Sheet 2, Datenminimierung auch Sheet 6, Zweckkompatibilität auch Sheet 4 (2/2)	(+)	(+) Datenminimierung S. 9, 14, 17 (+) Zweckbindung S. 6 f., 7 (Fragebogen), 8, 9, 14, 17	(+) Datenminimierung, S. 4 (+) Zweckbindung S. 3;
(+) S. 4, 5, 9,10, 11 (Checklisten)	(+) S. 2 f. *vgl. auch **Hamburger Thesen zum Personenbezug in Large Language Models**↗ v. 15.7.2024*	(+) Introduction	(–)	(+) S. 15 kurzer Satz im Zusammenhang mit Vertraulichkeit beim Training	(–)
(+) S. 4 und 9 (Checklisten)	(+) S. 2 (indirekt im Zusammenhang mit Personenbezug) und S. 4 (im Zusammenhang mit Diskriminierung)	(+) Sheet 4 (1/2 und 2/2), Sheet 8 (in consultation)	(+/–) nur allgemeine Bezugnahme	(+/–) vereinzelt kurze Bezugnahmen, dass es einer Rechtsgrundlage bedarf	(–)
(+) S. 9	(–)	(+) Sheet 3	(–)	(+/–) indirekt: Klärung der Zugriffsmöglichkeiten von Cloud-Anbietern S. 16; „Rollen- und Berechtigungskonzept“ S. 15,18,19	(+/–) S. 4 (nur knappe Bezugnahme auf Ermittlung der Verantwortlichkeit)
(+) Transparenz S. 7 (als Teil des „Datenschutz-Risikomodells“) (+) Infopflichten S. 5 (Checkliste)	(–)	(+) Sheet 2, Dokumentation in Sheet 7	(+)	(+) S. 5, 11 ff., 16 f.	(+) S. 3
(+) Auskunftsanspruch S. 5, 10 (Checkliste), Recht auf Löschung S. 6, 10 (Checkliste)	(–)	(–)	(+/–) nur allgemeine Bezugnahme auf Betroffenenrechte	(+) Auskunftsanspruch, S. 7; Betroffenenrechte allgemein S. 18 (in einem Satz)	(–)
(–)	(+) S. 22	(–)	(+)	(+) S. 5 (mehr oder weniger), S. 14 (Bezugnahme in einem Satz, indirekt), S. 18	(+) S. 3
(+), S. 7 (nur ein knapper Satz)	(–)	(+) Sheet 6 (Vorschrift wird nicht direkt genannt, aber Konzept DPbD wird beschrieben), Sheet 7	(–)	(+) S. 7 (analog?)	(+) S. 2, 4
(+) S. 4, 6, 9, 11 (Checklisten), S. 7	(+) S. 2	(+) Sheet 5	(–)	(+) S. 5	(+) S. 4

Weitere Informationen

DSK-Positionspapier „Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO)“, vom 03.05.24:
datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf

Datenschutzticker.de, 10.05.2024: DSK Orientierungshilfe für datenschutzkonformen Einsatz von KI:
datenschutzticker.de/2024/05/dsk-orientierungshilfe-fuer-datenschutzkonformen-einsatz-von-ki

„DSK Orientierungshilfe Künstliche Intelligenz und Datenschutz“ vom 6. Mai 2024:
datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

DSK-Pressemitteilung: datenschutzkonferenz-online.de/media/pm/2024-09-02_Klausurtagung_KI.pdf

Zum DSK Arbeitskreis KI:
www.baden-wuerttemberg.datenschutz.de/lfdi-uebernimmt-co-vorsitz-vom-dsk-arbeitskreis-ki

Orientierungshilfen für Verantwortliche vor Ort – Diskussionspapier und ONKIDA

Am 17. Oktober 2024 haben wir ein Update des im November 2023 erschienen Diskussionspapiers „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ vorgelegt. Das Papier soll verantwortlichen Stellen in Baden-Württemberg dabei helfen, sich mit den Rechtsgrundlagen auseinanderzusetzen, die das Datenschutzrecht für den Einsatz von Systemen der Künstlichen Intelligenz vorsieht. Das Datenschutzrecht definiert den Begriff der Künstlichen Intelligenz nicht. Unter dem in Wissenschaft und Praxis umstrittenen Begriff verstehen wir in diesem Papier – im Sinne einer denkbar weiten Arbeitsdefinition – alle Systeme des maschinellen Lernens. Vgl. dazu auch Art. 3 Nr. 1 KI-VO. Im Zuge der Überarbeitung des Diskussionspapiers (Version 2.0) wurden Rückmeldungen von Praktiker_innen sowie von Bürger_innen abgebildet, die sich an der Diskussion beteiligt haben. Einen besonderen Schwerpunkt bildete die Überarbeitung der Ausführungen zur Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f) DS-GVO (berechtigtes Interesse) sowie die Betrachtung einzelner Nutzungsszenarien, etwa im schulischen Bereich.

Mit dem Orientierungshilfen-Navigator KI & Datenschutz (ONKIDA) haben wir eine umfassende Fundstellenübersicht zu zehn zentralen Vorgaben des Datenschutzrechts in aufsichtsrechtlichen Orientierungshilfen zu Künstlicher Intelligenz erstellt, um einen schnellen Zugang zu ermöglichen.

Weitere Informationen

Diskussionspapier zu Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz 2.0:
www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

Ausführliche Auseinandersetzung mit dem Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/09/Beitrag_Diskussionspapier_Scheja_und_Partner.pdf

KI in der öffentlichen Verwaltung: Blick über den Tellerrand

KI kann in der öffentlichen Verwaltung nur eingesetzt werden, wenn keine Daten an externe Anbieter zur eigenen Nutzung übermittelt werden und eine Rechtsgrundlage für die Verarbeitung vorliegt. Die erste Anforderung, die Bürgerschaft u. a. davor schützt, dass ihre Daten zweckentfremdet werden, lässt sich häufig technisch und vertraglich lösen. Das Erfordernis einer Rechtsgrundlage stößt zumindest dann an Grenzen, wenn die Eingriffsschwere der Verarbeitung mehr als nur eine geringe Intensität aufweist. Die Generalklausel des § 4 LDSG BW ermöglicht öffentlichen Stellen des Landes die Verarbeitung personenbezogener Daten, soweit keine spezifische Rechtsgrundlage vorhanden ist („unbeschadet sonstiger Bestimmungen“) und keine eingriffsintensive Verarbeitung vorliegt (LT-Drs. 16 / 3930 S. 93). Soweit bereits Regelungen vorhanden sind, wie z. B. im Schulgesetz, in den Sozialgesetzbüchern oder in den §§ 13, 15 und 18 LDSG BW, kann die Generalklausel des § 4 LDSG regelmäßig nicht zur Anwendung kom-

men. Dies haben wir auch in unserem Diskussionspapier zu Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz 2.0 dargestellt.

Da die Schwelle für eingriffsintensive Verarbeitungen regelmäßig schnell erreicht ist, und um zudem Rechtssicherheit zu schaffen, wurde in Schleswig-Holstein bereits 2022 mit dem IT-Einsatz-Gesetz (ITEG) die Möglichkeit für den Einsatz von KI-Anwendungen in der öffentlichen Verwaltung geschaffen und seit November 2024 gilt in Hamburg das Verwaltungsdigitalisierungsgesetz (HmbVwDiG). Sowohl das ITEG als auch das HmbVwDiG ermöglichen den Einsatz von Systemen künstlicher Intelligenz bei öffentlichen Stellen (§ 2 ITEG, § 13 Abs. 1 HmbVwDiG) und auch für die Entwicklung und das Training von „datengetriebenen Informationstechnologien" bzw. Systemen künstlicher Intelligenz können personenbezogene Daten verarbeitet werden, wenn dies ohne diese Daten nur mit unverhältnismäßigem Aufwand oder gar nicht erreicht werden kann (§ 8 ITEG, § 13 Abs. 2 HmbVwDiG). Während das ITEG insbesondere die KI-Rüge als Ausgleich für den Eingriff in die informationelle Selbstbestimmung der Bürger_innen vorsieht, gibt es in dem HmbVwDiG keine über die DS-GVO hinausgehenden Bestimmungen. In Baden-Württemberg wird derzeit eine Überprüfung des Landesdatenschutzgesetzes unter diesen Gesichtspunkten durchgeführt. Dies begrüßen wir unter dem Aspekt der Rechtssicherheit und für den Schutz der personenbezogenen Daten der Bürger_innen sehr und stehen im Austausch mit den beteiligten Ressorts.

☛ Weitere Informationen

IT-Einsatz-Gesetz Schleswig-Holstein, ITEG:
gesetze-rechtsprechung.sh.juris.de/bssh/document/jlr-ITEGSHrahmen

Verwaltungsdigitalisierungsgesetz Hamburg, HmbVwDiG:
buergerschaft-hh.de/parldok/dokument/87927

KI im Ländle: F13

Das oben Gesagte gilt auch für F13, die vom Land Baden-Württemberg entwickelte KI-basierte Textassistenz für den Einsatz im Webbrowser. Diese KI-basierte Textassistenz kann als Chatbot, als Rechercheassistenz zu landespolitischen Themen, zur Generierung von Textzusammenfassungen sowie zur Erstellung von Vermerken eingesetzt werden. Die dafür genutzte Infrastruktur befindet sich vollständig in der Verantwortung und im Zugriffsbereich des Landes Baden-Württemberg – eine zwingende Voraussetzung, um einen Datenabfluss an Dritte und einen damit möglicherweise verbundenen Kontrollverlust über die Daten zu verhindern. Die eingesetzten KI-Modelle werden dabei nicht unmittelbar mit den Daten aus der Verwaltung trainiert, sondern es wird eigens für das System eine Wissensdatenbank erstellt und eingesetzt, die mit Dokumenten aus der Verwaltung gefüllt wird. Das KI-basierte Sprachmodell generiert aus den Eingaben in den Chatbot und den daraus resultierenden Suchergebnissen aus der Wissensdatenbank eine Antwort, die sich so weit wie möglich aus der Wissensdatenbank ergibt. Dadurch sollen insbesondere halluzinierte, d. h. „erfundene" Antworten der KI vermieden werden. Die eingesetzten KI-Modelle werden nicht mit den personenbezogenen Daten aus der Verwaltung (nach-)trainiert, also das KI-Modell wird nicht mit personenbezogenen Daten aus der baden-württembergischen Verwaltung gefüttert. Das vereinfacht den Umgang mit den Rechten der Betroffenen erheblich, da etwas, was nicht im KI-Modell vorhanden ist, beispielsweise auch nicht gelöscht werden muss. Eine Löschung in der selbst geschaffenen und befüllten Wissensdatenbank ist andererseits einfach umsetzbar.

Datenschutz durch KI-Gestaltung ist unverzichtbarer Baustein digitaler Souveränität. Was man sich immer wieder klarmachen muss: Bei einigen, wenn nicht vielen KI-Anwendungen wird regelmäßig von einer geringen Eingriffsintensität auszugehen sein. KI-Anwendungen unterliegen jedoch immer einer Risikoabwägung im Einzelfall. Welche Relevanz der Personenbezug im KI-Modell hat, in welcher Art besondere Kategorien personenbezogener Daten im Modell und in der Anwendung verarbeitet werden, ob Betroffenenrechte im KI-Modell umgesetzt werden können und wer als verantwortliche Stelle dies im Blick haben muss, sind nur einige der Fragen, die berücksichtigt werden müssen (siehe

auch „EDPB opinion on AI models: GDPR principles support responsible AI“ vom 18. Dezember 2024 und „DSK Orientierungshilfe Künstliche Intelligenz und Datenschutz“ vom 6. Mai 2024). Digitalisierung ist ein permanenter Prozess. Und dies bedeutet: Es reicht nicht, eine Anwendung einmalig zu betrachten, sondern sie ist permanent im Blick zu behalten und dabei muss insbesondere immer wieder berücksichtigt werden, wenn sich technisch etwas ändert.

Weitere Informationen

Pressemitteilung der Landesregierung, Baden-Württemberg geht neue Wege bei Verwaltungs-KI, 12.11.2024: stm.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/baden-wuerttemberg-geht-neue-wege-bei-verwaltungs-ki

Stuttgarter Zeitung, Was kann die Verwaltungs-KI wirklich?, 20.09.2024: stuttgarter-zeitung.de/inhalt.f13-was-kann-die-verwaltungs-ki-wirklich.0277706f-e1ec-4c38-9f1c-5ad6c76a-b53e.html

„EDPB opinion on AI models: GDPR principles support responsible AI“, vom 18. Dezember 2024: edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_en

Kohärentes Daten- und Digitalrecht – Lost in Interplays

Angesichts der Fülle von Neuerungen im europäischen Digital- und Datenrecht wünscht sich der Rechtsanwender mehr Klarheit und Rechtssicherheit. Ausgehend von der Erkenntnis, dass KI-VO und DS-GVO künftig parallel anwendbar sein werden, stellen sich zur Wechselwirkung der beiden Regelwerke viele Fragen („interplay issues“). Das gilt namentlich für diejenigen Sachverhalte, die in der gemeinsamen Schnittmenge der Verordnungen angesiedelt sind, die also sowohl KI-Systeme / Modelle im Anwendungsbereich der KI-VO betreffen als auch die Verarbeitung personenbezogener Daten im Anwendungsbereich der DS-GVO zum Gegenstand haben. Künftig näher erörterungsbedürftig ist in diesem Kontext u. a. beispielsweise die Frage, wie weit die Befugnis zur Datenverarbeitung i. S. d. Art. 10 Abs. 5 KI-VO reicht, wie das Gebot menschlicher Aufsicht (Art. 14 KI-VO) und Artikel 22 DS-GVO zusammenwirken, welche Synergien es ggf. zwischen nach DS-GVO gebotener Datenschutzfolgenabschätzung und Grundrechtsfolgenabschätzung nach KI-VO gibt und ob es Unterschiede in den Transparenzanforderungen zwischen den beiden Regelungskreisen gibt. Die Rechtsfragen werden in Arbeitsgruppen des Europäischen Datenschutzausschusses erörtert, bei denen wir aktiv mitarbeiten.

Forschung und Gesundheitsdaten

In der Entscheidungspraxis der DSK spielten 2024 die Forschung und Gesundheitsdaten eine gewichtige Rolle. Dass es sich bei Gesundheitsdaten um besonders sensible Daten mit entsprechend hohem Schutzbedarf handelt, was technisch und organisatorisch über den gesamten Lebenszyklus der Verarbeitung abgebildet werden muss, unterstrich die DSK in ihrer Entschließung vom 15. Mai 2024 zum besseren Schutz von Patient_innendaten bei Schließung von Krankenhäusern.

Breiten Raum in der Befassung der DSK im letzten Jahr nahm der Umgang mit Gesundheitsdaten im besonderen Verarbeitungskontext der Forschung ein. Die bereits 2022 in der „Petersberger Erklärung“ der Datenschutzkonferenz niedergelegten Grundsätze zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung wurden durch ein Positionspapier zum Begriff des „wissenschaftlichen Forschungszwecks“ sowie einen Beschluss zu genetischen Daten weiter konkretisiert. Im Beschluss vom 11. September 2024 setzte sich die DSK intensiv mit dem Begriff des wissenschaftlichen Forschungszwecks auseinander, der in der DS-GVO an verschiedener Stelle geregelt ist und für Datenverarbeitungen unter Ägide des Forschungsprivilegs Vorgaben enthält, die der ebenfalls grundrechtlich geschützten Forschungsfreiheit und dem damit verbundenen Beitrag für das Gemeinwohl in einem europäischen Raum der Forschung Rechnung tragen (Art. 13 GRCh; Art. 179 Abs. 1 AEUV; ErwG 159 DS-GVO).

Gesundheitsforschung

„Petersberger Erklärung“ der DSK zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, vom 24.11.2022:
datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Zentrale Punkte der Erklärung, die darauf abzielt, der Bedeutung wissenschaftlicher Forschung mit Gesundheitsdaten ebenso Rechnung zu tragen, wie den Schutz besonders sensibler personenbezogener Daten zu gewährleisten, sind unter anderem die Forderung nach Transparenz und Nachvollziehbarkeit der Datenverarbeitungsprozesse für die betroffenen Personen. Empfohlen wird die möglichst aktive Einbindung der betroffenen Personen, auch wenn die Datenverarbeitung auf gesetzlicher Grundlage erfolgt. Damit korrespondiert ein Vorschlag zur Implementierung digitaler Managementsysteme für verbesserte Informations-, Kontroll- und Mitwirkungsmöglichkeiten. Gefordert werden weiter einheitliche, länderübergreifende Regelungen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken sowie eine lückenlose Überwachung und Durchsetzung datenschutzrechtlicher Regelungen durch unabhängige Datenschutz-Aufsichtsbehörden. Besonders betont schließlich wird die Notwendigkeit eines Forschungsgeheimnisses zum Schutz personenbezogener medizinischer Forschungsdaten. Schlüsselgrundsatz des Papiers ist schließlich die Aussage: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen (bspw. Verschlüsselung, Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung), desto umfangreicher und spezifischer können die Daten genutzt werden („Petersberger Maxime“).

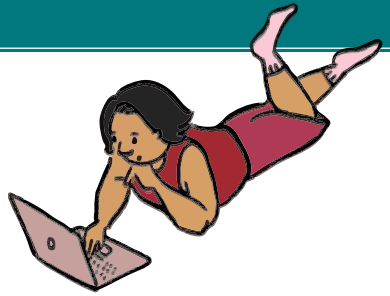
DSK-Positionspapier zum Begriff „wissenschaftliche Forschungszwecke“, vom 11.9.2024:
datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf

Wo in der DS-GVO ist der Begriff „wissenschaftliche Forschungszwecke geregelt?

Art. 5 Abs. 1 Buchst. b) DS-GVO (Zweckbindung), Art. 9 Abs. 2 Buchst. j) DS-GVO (Öffnungsklausel für die Verarbeitung besonderer Kategorien personenbezogener Daten), Art. 14 Abs. 5 Buchst. b) DS-GVO (Einschränkung der Informationspflichten), Art. 17 Abs. 3 Buchst. d) DS-GVO (Einschränkung des Rechts auf Löschung), Art. 21 Abs. 6 DS-GVO (Widerspruchsrecht) und Art. 89 DS-GVO (besondere Garantien und Ausnahmen).

DSK-Positionspapier „Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken“, vom 15.05.2024:
datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf

„Genetische Daten“ sind nach Art. 4 Nummer 13 DS-GVO personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.



© Illustration: Y. Dwiputri

Die DS-GVO ermöglicht Forschung und Innovation.

☛ Weitere Informationen

DSK in ihrer Entschließung vom 15.05.2024 zum besseren Schutz von Patientendaten bei Schließung von Krankenhäusern: datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf

Datenschutz im Parlament

Der Europäische Gerichtshof hat am 16. Januar in der Rechtssache C-33 / 22 (Österreichische Datenschutzbehörde) ein Urteil gefällt, das die bereits zuvor angelegte Linie des Gerichts (EuGH, Rs. C-272 / 19 vom 9. Juli 2020) bestärkt und gravierende Auswirkungen für alle Parlamente der Mitgliedstaaten der Europäischen Union hat. In dem Vorlageverfahren ging es um die Frage, ob die DS-GVO auch auf parlamentarische Untersuchungsausschüsse anwendbar ist und wer die Aufsicht über die Durchsetzung der DS-GVO in Parlamenten ausübt. Kurz gesagt interpretiert der EuGH den Anwendungsbereich des Unionsrechts und der DS-GVO weit und bezieht den parlamentarischen Bereich explizit mit ein.

Für die Situation in Baden-Württemberg bedeutet das im Grundsatz, dass die DS-GVO für den Landtag anwendbar ist und auch die Regelungen über die Zuständigkeit, die Aufgaben und die Befugnisse der Datenschutzaufsicht gelten. Zugleich weist der EuGH in seinem oben genannten Urteil aber darauf hin, dass der nationale Gesetzgeber (landes-)verfassungsrechtlichen Besonderheiten durchaus Rechnung tragen kann: Art. 51 Abs. 1 DS-GVO räumt „jedem Mitgliedstaat einen Ermessensspielraum ein, der es ihm ermöglicht, so viele Aufsichtsbehörden einzurichten, wie insbesondere aufgrund seiner verfassungsmäßigen Struktur erforderlich sind“ (EuGH, RS C-33 / 22, Rn. 69). Die

Schaffung einer speziellen Aufsichtsbehörde zur Überwachung des Datenschutzes im Parlament ist damit möglich. Was die konkrete Ausgestaltung angeht, sind externe und interne Modelle denkbar. Das einzurichtende Datenschutzgremium als spezifische Aufsichtsstelle müsste jedenfalls zentralen Vorgaben der Art. 52 ff. DS-GVO Rechnung tragen (zu den Voraussetzungen Hansen / Keber / Roßnagel, in: FAZ vom 1. Mai 2024).

☛ Weitere Informationen

Souveränität und Datenschutzaufsicht, Marit Hansen, Tobias Keber, Alexander Roßnagel, FAZ vom 01.05.2024: faz.net/einspruch/souveraenitaet-und-datenschutzaufsicht-19690907.html

Haushaltssituation

Zur Bewältigung der anstehenden Herausforderungen in einem hochdynamischen, technikgetriebenen Umfeld und im Rahmen einer immer komplexer werdenden Rechtslage hatten wir eine angemessene Verstärkung der Personalausstattung angemeldet. Im Zuge der abschließenden Beratungen über den Regierungsentwurf wurden wir gebeten, diese Stellenmehrbedarfe im parlamentarischen Verfahren zu verfolgen. Mit unserem Schreiben an die Vorsitzenden der im Landtag von Baden-Württemberg vertretenen Fraktionen vom 2. Oktober 2024 ist der notwendige Stellenmehrbedarf mit detaillierter Begründung dargelegt worden. Leider blieb diese Initiative ohne Erfolg, sodass wir künftig einem deutlichen Zuwachs an Aufgaben und deren Komplexität mit einem reduzierten Personalkörper zu begegnen haben.

Fazit

Rückblickend ist für das vergangene Datenschutzjahr eine politische Großwetterlage zur Kenntnis zu nehmen, in dem der Datenschutz seine Daseinsberechtigung und Anschlussfähigkeit mehr denn je zu beweisen hat. Dabei werden die negativen Folgen unregulierter Technisierung bis hin zu möglichen Auswirkungen für unsere demokratische Gesellschaft medial stark diskutiert. Datenschutz ist Stütze unserer Demokratie. Dass Datenschutz mit der Intensivierung digitaler Datennutzung mitwachsen muss, sollte sich fast von selbst verstehen, wenn man vertrauenswürdige künstliche Systeme bauen und anwenden will. Informationelle Selbstbestimmung und Innovation sind keine Gegenspieler, sondern Ausdruck unseres gesellschafts- und damit auch rechtspolitischen Selbstverständnisses. Im Zentrum des technischen Fortschritts muss der Mensch stehen. Gesichert wird dies durch eine wertebasierte Regulierung von Künstlicher Intelligenz ebenso wie durch einen grundrechtssensiblen Umgang mit personenbezogenen Daten. Für Normadressaten und Aufsichtsbehörden gleichermaßen herausfordernd ist, den bis dato wenig kohärenten Kanon des Digital- und Datenrechts für Europas digitale Dekade zu durchdringen.

© Illustration: Y. Dwiputri

ABSCHNITT 1

Kooperation, inhaltliche Schwerpunkte, Schulungen und Kommunikation

Die europäische DS-GVO ist die rechtliche Übersetzung der Werte und Normen der europäischen Gesellschaften.

Viel Bewegung in Deutschland und Europa – Die Stabsstelle für Deutsche und Europäische Zusammenarbeit

Die Arbeit der Stabsstelle für Deutsche und Europäische Zusammenarbeit war auch im Berichtsjahr 2024 wieder durch eine bunte Aufgabenvielfalt geprägt. Auf Ebene der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) gleichermaßen wie auf Ebene des Europäischen Datenschutzausschusses (EDSA) und seiner Arbeitsgruppen war das Thema Künstliche Intelligenz von dem Blick in Richtung Praxis und Umsetzung geprägt, um nicht nur Zuständigkeiten zu klären, sondern auch konkrete Hilfestellung für verantwortliche Stellen zu geben. Dasselbe gilt für die Vielzahl an neuen digitalen Rechtsakte der Europäischen Union. Beide Themenkomplexe wurden im Tätigkeitsbericht 2023 bereits dargestellt und sollen im aktuellen Berichtszeitraum akzentuiert beleuchtet werden. Und auch die Arbeit an Grundsatzthemen und grundlegenden Festlegungen nimmt immer weiter an Fahrt auf. Die nunmehr eineinhalb Jahre enge Zusammenarbeit und Koordinierung der Fragen im Grundsatzbereich im Kontext nationaler wie europäischer Entwicklungen mit der neuen Hausleitung haben der Stabsstelle hier die Setzung neuer Schwerpunkte sowie thematische Fortentwicklung ermöglicht.

Die Arbeit der Stabstelle ist umfangreich. Sie erstellt Stellungnahmen, befasst sich mit Prüfungen, erarbeitet FAQ (Art. 57 Abs. 1 Buchst. b) und d)), sorgt für die Kooperation mit dem EDSA und der DSK (Art. 57 Abs. 1 Buchst. g) und t)) und hat auf europäischer Ebene die digitalen Rechtsakte im Blick (Art. 57 Abs. 1 Buchst. i)).

Die Arbeit der DSK

Auch im Jahr 2024 hatte die DSK eine Vielfalt datenschutzrechtlicher Themen im Blick. Begleitet

von 13 Pressemitteilungen veröffentlichte sie im Berichtsjahr insgesamt drei Entschließungen, fünf Beschlüsse, drei Orientierungshilfen und einen Anwendungshinweis zu aktuellen und relevanten Themen aus der Welt der Datenschutzaufsicht. Unsere Stabsstelle für Deutsche und Europäische Zusammenarbeit ist koordiniert und bereitet die Sitzungen der DSK vor und unterstützt die Hausleitung in diesem Bereich unmittelbar.

Infokasten

Entschließungen sind öffentliche Stellungnahmen zu datenschutzpolitischen Fragen.

Beschlüsse sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen.

Orientierungshilfen und Standardisierungen sind fachliche Anwendungshilfen für Verantwortliche, Auftragsverarbeiter, Herstellerinnen und Hersteller und die Öffentlichkeit.

Die KI braucht uns!

Die Benennung der zuständigen Aufsichtsbehörde für die Marktüberwachung und Kontrolle von KI-Systemen ist politisch nach wie vor ungeklärt. Während sich die Bundespolitik klar für die Bundesnetzagentur als Marktüberwachungsbehörde ausspricht (Tagesspiegel, AI-Act-Umsetzung: Noch viele offene Fragen, 7. August 2024), sieht die KI-VO die bereits benannten Datenschutzaufsichtsbehörden als Marktüberwachungsbehörde für biometrische KI-Systeme, Strafverfolgung, Wahlen, Migration, Asyl, Grenzkontrolle, Rechtspflege und demokratische Prozesse vor. Bereiche also, die ohnehin durch die Verarbeitung (besonderer Kategorien) personenbezogener Daten geprägt sind und der Datenschutzaufsicht der Länder und des Bundes in ihrer jeweiligen Zuständigkeit unterliegen.

Bereits am 3. Mai 2024 hat sich die DSK dafür ausgesprochen, die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und die Datenschutzaufsichtsbehörden der Länder als Marktüberwachungsbehörden der KI-VO zu bestimmen (DSK, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), 3. Mai 2024):
» *Wird ein KI-System bundesweit als Produkt angeboten oder aus dem internen Gebrauch heraus zum externen Vertrieb auf den Markt gebracht, liegt die Zuständigkeit hierfür beim Bund. Insbesondere die Nutzung oder die Entwicklung von KI-Systemen für den internen Gebrauch durch Unternehmen und Behörden wird von den Landesdatenschutzaufsichtsbehörden bzw. der Bundesdatenschutzbehörde in ihrer jeweiligen Zuständigkeit überwacht.* «

Diese Position greift der EDSA in einer Stellungnahme vom 16. Juli 2024 ebenfalls auf (EDSA, Statement 03 / 2024 on data protection authorities' role in the Artificial Intelligence Act framework, 16. Juli 2024) und unterstützt damit aktiv die bereits von der DSK deutlich geäußerte Forderung.

Wenn die Bundesministerien die Bundesnetzagentur als Marktüberwachungsbehörde vorsehen, die nach der JI-Richtlinie neu zu benennen wäre, wird verkannt, dass Art. 74 KI-VO hierfür keine Öffnungsklausel vorsieht und die bereits benannten Aufsichtsbehörden vorgesehen sind (Roßnagel, Editorial, NJW-aktuell 41 / 2024). Zudem gilt für eine produktregulierende Verordnung, wie die KI-VO eine ist, und insbesondere für den öffentlichen Bereich, dass diese grundsätzlich dem Landesrecht unterliegt und nur zur einheitlichen Regelung bundesweiter Sachverhalte eine Bundesbehörde zuständig sein kann (Art. 83, 72 Abs. 2 GG; DSK, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO), 3. Mai 2024). Für eine andere Regelung wäre indes die Notwendigkeit einer Verfassungsänderung zu prüfen (vgl. Martini / Botta, MMR 2024, 630, 635).

Unabhängig von diesen rechtlichen Fragen sind die Datenschutzaufsichtsbehörden ohnehin für datenschutzrechtliche Belange im Zusammenhang mit KI zuständig. Die Benennung einer weiteren Aufsichtsbehörde würde gerade nicht dem vom

Bund geäußerten Ziel dienen, die Zahl der beteiligten Aufsichtsbehörden zu reduzieren und die Aufsichtsstruktur zu verschlanken. Die DS-GVO umfasst nach Art. 2 Abs. 1 den Schutz aller Grundrechte und Grundfreiheiten, zu denen das Recht auf Schutz personenbezogener Daten, aber auch z. B. die unternehmerische Freiheit gehören. Eine Abwägung insbesondere dieser beiden genannten Grundrechte zu treffen, ist Teil der langjährigen Praxis der datenschutzrechtlichen Aufsicht und muss auch weiterhin aus einer Hand erfolgen, um den Unternehmen, aber auch den betroffenen Bürger_innen weiterhin Rechtssicherheit und Schutz zu bieten.

Eine Benennung der Datenschutzaufsichtsbehörden als Marktüberwachungsbehörden nach der KI-VO ist aus Sicht der Datenschutzaufsichtsbehörden die einzige Lösung, um sowohl die Aufsichtsstruktur in Deutschland nicht zu vergrößern als auch die Rechte und Freiheiten der betroffenen Unternehmen und Bürger_innen effektiv zu schützen.

☛ Weitere Informationen

DSK, Nationale Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO) vom 03.05.2024
datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf

EDSA, Statement 03 / 2024 on data protection authorities' role in the Artificial Intelligence Act framework vom 16.07.2024
edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf

BDSG-neu – aber bitte richtig!

Eine weitere wichtige Stellungnahme der DSK ist die vom 12. April 2024 zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes. Diesen Gesetzentwurf (BT-Drs. 20 / 10859, Februar 2024) hat die DSK zum Anlass genommen, sich zu wichtigen Punkten aus dem Entwurf und einem weitergehenden Regelungsbedarf zu äußern. Ein besonderes Anliegen war es zunächst, nochmals den Bedarf der Institutionalisierung der DSK hervorzuheben, um der Bedeutung des Gremiums und der Unabhängigkeit der Datenschutzaufsichtsbehörden des Bundes und der Länder gerecht zu werden. Dazu gehört v. a. auch die Einrichtung einer eigenen ständigen Geschäftsstelle zur organisatorischen Unterstützung. Die vorgeschlagene Verankerung im Gesetz ist grundsätzlich zu begrüßen, bedarf nach Ansicht der deutschen Datenschutzaufsichtsbehörden jedoch genauerer Regelungen hinsichtlich der Zielsetzung der DSK, um einen Mehrwert zu dem ohnehin bereits bestehenden und jahrelang erprobten Kooperationssystem zu erreichen. Darüber hinaus geht die DSK in ihrer Stellungnahme auf vorgeschlagene zusätzliche Zuständigkeitsregelungen ein und erklärt hierzu deutlichen Konkretisierungsbedarf oder empfiehlt zum Teil sogar die Streichung einzelner vorgeschlagener Regelungen des Gesetzesentwurfs, um eine unnötige Über-, wenn nicht Fehlregulierung zu vermeiden. Beispielhaft sei hierzu die vorgeschlagene Regelung im Bereich der gemeinsamen Verantwortlichkeit genannt, die mangels ausreichender Genauigkeit mehr Verwirrung als Rechtsklarheit stiften dürfte. Einen weiteren Schwerpunkt der Stellungnahme bildet der von der DSK formulierte Anpassungsbedarf hinsichtlich bestehender wie neuer Vorschriften zum Bußgeldverfahren. Auf unseren ausdrücklichen Wunsch wurde hierbei auch speziell die Forderung an den Gesetzgeber aufgenommen, den Bußgeldstellen der Datenschutzaufsichtsbehörden eine Befugnis zur Einziehung und erweiterten Einziehung von Gegenständen einzuräumen, um ihnen eine stärkere Durchsetzungskraft zu verschaffen. Schließlich äußerte sich die DSK weiterhin zu bereichsspezifischen Regelungen des Gesetzentwurfs wie Scoring, Geschäftsgeheimnissen im Zusammenhang mit Auskunftsansprüchen und Religionsgemeinschaften.

☛ Weitere Informationen

Stellungnahme der DSK vom 12. April 2024 zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes
datenschutzkonferenz-online.de/media/st/240412_BDSG-E_Stellungnahme_DSK.pdfs

Der EDSA spricht

Die Entwicklungen der vergangenen Jahre, über welche die Stabsstelle für Deutsche und Europäische Zusammenarbeit auch regelmäßig berichtet, machen deutlich, dass der EDSA eine immer wichtigere Rolle einnimmt und einen zentralen Einfluss auf relevante Diskussionen und Problemstellungen im Bereich des Datenschutzrechts hat. Der Zusammenschluss aller Aufsichtsbehörden der Europäischen Mitgliedstaaten erarbeitet vermehrt Stellungnahmen und Leitlinien, die richtungsweisend für die praktische Anwendung wie Umsetzung der DS-GVO und auch Grundlage für die Arbeit der Datenschutzaufsicht sind. Die Stabsstelle betreut die Arbeit des EDSA durch die Teilnahme und Beobachtung der Tätigkeiten der Experten-Arbeitsgruppen sowie des Plenums.

Update zu CSAM – Child Sexual Abuse Material

Der Missbrauch von Kindern und die Verbreitung expliziter Darstellungen dieses Verhaltens müssen mit allen rechtlichen Mitteln bekämpft werden. Darüber haben wir unter anderem im Tätigkeitsbericht 2022 berichtet (Abschnitt 4.5). Die Tatsache, dass die gewählten Mittel verhältnismäßig und geeignet sein müssen und zudem die Grundrechte auf Privatsphäre und Datenschutz zu beachten sind, macht die Wahl dieser Mittel zu einer besonders anspruchsvollen Aufgabe. In seiner Stellungnahme 01 / 2024 nimmt der EDSA Bezug auf den Standpunkt des Europäischen Parlaments vom 13. November 2023 zur Regelung von CSAM.

In der Stellungnahme vom 13. Februar 2024 äußerst sich der EDSA erneut zu der Problematik und hebt insbesondere den Verzicht auf Maßnahmen hervor, die zu einer Verschlechterung der Sicherheit durch Ende-zu-Ende-Verschlüsselung geschützter Verbindungen führen würden. Wichtig ist hierbei die nun erfolgte Klarstellung des Europäischen Parlaments, dass die Regelungen zu CSAM in keiner Weise als Verbot, Einschränkung oder Untergrabung der Ende-zu-Ende-Verschlüsselung verstanden oder ausgelegt werden dürfen (ErwG. 9a und Art. 6a CSAM; europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html). Dennoch bestehen nach wie vor Bedenken hinsichtlich einer zu generellen und wahllosen Überwachung privater Kommunikation (Art. 7 CSAM) und hinsichtlich der Erkennung „neuer" CSAM. Problematisch ist hier insbesondere die nach wie vor hohe Rate von false positive Ergebnissen.

© kwasibanane

Mit seiner Digitalstrategie läuft die EU vorne mit bei der Regulierung und dem Nutzen von digitalen Anwendungen.

Der vom Europäischen Parlament eingeschlagene Weg ist zu begrüßen. Aus datenschutzrechtlicher Sicht besteht allerdings noch weiteres Potential, um die Bürger_innen vor einer nicht zielgerichteten Überwachung mit potentiell gravierenden Folgen für falsch Verdächtigte zu schützen.

Europas „digitale Dekade" befeuert interdisziplinäre Kooperationen

Die EU-Digitalstrategie sorgt nicht nur dafür, dass sich Datenschutzaufsichtsbehörden inhaltlich mit den dazugehörigen Rechtssetzungsakten beschäftigen müssen. Vielmehr besteht zunehmend das – zum Teil in verschiedenen Regelungen, zum Teil durch Rechtsprechung statuierte – Erfordernis, dass Behörden interdisziplinär kooperieren (siehe hierzu bereits unseren Bericht aus dem vergangenen Jahr, S. 12 ff.). Insbesondere wird eine verstärkte Zusammenarbeit zwischen Datenschutz-, Wettbewerbs- und Verbraucherschutzbehörden sowie den entsprechenden Gremien immer wichtiger. Unsere Stabsstelle engagiert sich in der „Taskforce Consumer & Competition" des EDSA, die mit dem Regulierungsdialog zwischen diesen Rechtsbereichen betraut ist.

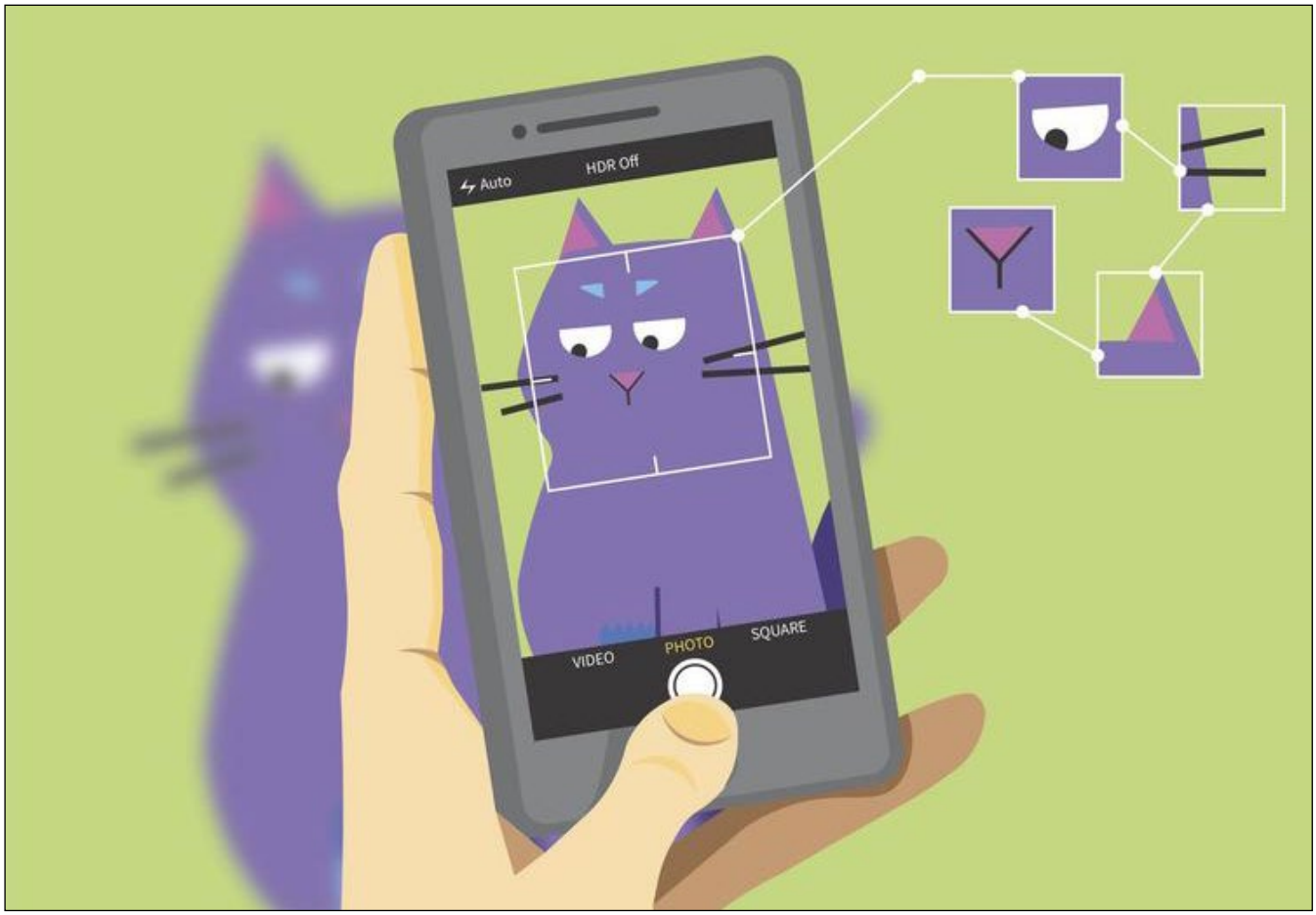
Unter unserer Federführung wurde ein FAQ-Dokument zur Zusammenarbeit zwischen den Behörden und Gremien aus den Bereichen Datenschutz, Wettbewerb und Verbraucherschutz („Frequently Asked Questions on cooperation with competition and consumer protection authorities") erstellt, um die nationalen Datenschutzaufsichtsbehörden bei der Umsetzung von Kooperationen zu unterstützen und bereits in einigen Mitgliedstaaten bestehende Best Practices zu diesem Thema zu fördern. Die FAQ wurden am 27. März 2024 bei der Expertengruppe zur Strategieberatung des EDSA (Strategic Advisory Expert Subgroup) von uns vorgestellt. Die Stabstelle hat auch hier herausragende Arbeit geleistet und gezeigt, dass wir aus Baden-Württemberg heraus die europäische Entwicklung beim Datenschutz gestalten können. In den FAQ wird unter anderem untersucht, welche unterschiedlichen Formen der Zusammenarbeit in den einzelnen EU-Mitgliedstaaten bereits existieren.

Während sich die Zusammenarbeit in einigen Mitgliedstaaten auf den „Bedarfsfall" und Ad-hoc-Konsultationen beschränkt, bestehen in anderen rechtliche Vorgaben zur Kooperation. Zunehmend kooperieren Behörden auch auf freiwilliger Basis. Nachdem sich in Frankreich die Datenschutz- und die Wettbewerbsaufsicht schon am 12. Dezember 2023 mit einer gemeinsamen Absichtserklärung zur verstärkten Zusammenarbeit aus dem Jahr verabschiedeten, startete auf Bundesebene das „Digital Cluster Bonn" mit der medienwirksamen Unterzeichnung eines „Memorandum of Understanding" am 15. Januar 2024. Gemeinsam erstellte Kooperationsprotokolle, Absichtserklärungen oder ähnliche Vereinbarungen sind nicht zwingend rechtsverbindlich, können aber die Modalitäten für eine gute Zusammenarbeit regeln.

Eine regelmäßige, koordinierte und strukturierte Zusammenarbeit verschiedenster Institutionen – auch auf freiwilliger Basis – zur verwaltungseffizienten, einheitlichen Handhabung der neuen EU-Digitalrechtsakte sowie zur Schaffung von Synergien ist sehr zu begrüßen. Ob Absichtserklärungen das geeignete Mittel dafür sind, feststellbare Ergebnisse durch die Kooperationen zu erzielen, wird sich jedoch in Zukunft zeigen müssen.

Von der Ambivalenz partnerschaftlicher Zusammenarbeit mit der Europäischen Kommission

Die Arbeit der „Taskforce Consumer & Competition" gerät bei ihren Tätigkeiten regelmäßig ins Visier der Europäischen Kommission. Nachdem die Taskforce einen Leitfaden zum Zusammenspiel des Gesetzes über digitiale Märkte („Digital Markets Act", kurz: DMA) und der DS-GVO entworfen hatte, zeigte sich die EU-Kommission in einem Schreiben an den Vorsitz des EDSA besorgt darüber, dass der EDSA seine Kompetenzen überschreite, denn Leitlinien zum DMA kann gemäß Artikel 47 DMA die Kommission erlassen. Nun soll – ganz im Sinne der interdisziplinären Kooperation – an gemeinsamen Leitlinien gearbeitet werden. „Joint Guidelines on the Interplay between DMA and GDPR" sind einerseits eine Chance, qualitative Leitlinien zu veröffentlichen, die Einheitlichkeit der Rechtsauslegung durch die EU-Kommission und Datenschutzaufsichtsbehörden zu fördern und eine große Aufmerksamkeit zu erlangen.



Europa befasst sich intensiv mit neuen digitalen Technologien.

Andererseits bilden Kooperationsprodukte stets einen Kompromiss ab. Gemeinsame Leitlinien bergen mithin die Gefahr, dass die Datenschutzaufsichtsbehörden in ihrer Unabhängigkeit nach Art. 52 DS-GVO tangiert werden. Die Ergebnisse dieser Kooperationsverhältnisse bleiben abzuwarten. In den neuen Digitalrechtsakten der EU zeichnet sich grundsätzlich ab, dass Kooperationsmechanismen von Gesetzes wegen durch Gremienarbeit (so ist es im DMA z. B. die „hochrangige Gruppe", Art. 40 DMA) etabliert werden sollen. Auch anderen Aufsichtsbehörden könnte bei näherer Betrachtung auffallen, dass die Machtverteilung kontrakooperativ zugunsten der Kommission auszufallen scheint.

To pay or not to pay

Am 17. April 2024 erließ der EDSA eine Stellungnahme zu Pay oder Consent Modellen auf großen Online-Plattformen, nachdem die Datenschutzaufsichtsbehörden aus Hamburg, Norwegen und den Niederlanden diese gemäß Art. 64 Abs. 2 DS-GVO beantragt hatten. Die Stellungnahme beschäftigt sich mit der Gültigkeit der Einwilligung zur Verarbeitung personenbezogener Daten für verhaltensbasierte Werbung im Rahmen solcher Pay oder Consent Modelle. Wenn Bürger_innen auf großen Online-Plattformen unterwegs sind, laufen ihnen heute solche Modelle über den Weg, die in der Regel zwei Alternativen beinhalten: Entweder geben die Nutzenden all ihre Daten preis, oder sie müssen für die Nutzung des Dienstes bezahlen.

Der EDSA kommt in seiner Stellungnahme zu dem Ergebnis, dass dies in den meisten Fällen nicht die Anforderungen an eine gültige datenschutzrechtliche Einwilligung erfüllt, da den Nutzenden keine echte Wahlmöglichkeit geboten wird. Anstatt lediglich eine kostenpflichtige Alternative anzubieten, sollten die Verantwortlichen ihren Nutzenden vielmehr eine – weitere – gleichwertige Alternative anbieten, die kostenlos ist und dennoch nicht mit ver-

haltensbasierter Werbung einhergeht. Basierend auf den Grundsätzen aus Art. 5 DS-GVO sollten die Anbieter der Plattformen zudem die Notwendigkeit und Höhe der geforderten Gebühr sowie mögliche negative Folgen für die Betroffenen bei verweigerter Einwilligung berücksichtigen.

Wir begrüßen den Kurs des EDSA, den Schutz der Nutzenden und ihrer personenbezogenen Daten auf großen Online-Plattformen durch immer mehr Entscheidungen weiter zu stärken. Es wird jedoch abzuwarten sein, ob die Stellungnahme so Bestand haben wird. Die Zulässigkeit und Reichweite entstehender Eingriffe in den Markt und in Geschäftsmodelle durch auf datenschutzrechtliche Erwägungen gestützte Entscheidungen kann durchaus diskutiert werden. Der Konzern Meta beantragt vor dem Europäischen Gerichtshof u. a. aus diesem Grund aktuell die Aufhebung der Stellungnahme des EDSA.

☛ **Weitere Informationen**

Stellungnahme zu Pay or Consent Modellen
edpb.europa.eu/system/files/2024-04/edpb_opinion_202408_consentorpay_en.pdf

Was lange währt … Leitlinien zum berechtigten Interesse

Am 8. Oktober 2024 verabschiedete der EDSA nach jahrelanger Arbeit, an der auch wir aktiv beteiligt waren, die allseits lang ersehnten Leitlinien zur Verarbeitung personenbezogener Daten auf Grundlage von Art. 6 Abs. 1 Buchst. f) DS-GVO. Die Leitlinien beleuchten das berechtigte Interesse als eine der möglichen Rechtsgrundlagen gemäß Art. 6 Abs. 1 DS-GVO – und geben damit Hilfestellung zu der in der Praxis wohl am häufigsten genutzten wie auch am stärksten umstrittenen Rechtsgrundlage.

Die Leitlinien geben Aufschluss über die einzelnen Kriterien, die Verantwortliche erfüllen müssen, um personenbezogene Daten auf der Grundlage eines berechtigten Interesses rechtmäßig verarbeiten zu können. Dabei werden auch jüngste zugehörige Urteile des EuGH (wie beispielsweise Az. C-621 / 22, 4. Oktober 2024) berücksichtigt.

Die Leitlinien stellen klar, dass Verantwortliche bei einer Verarbeitung gestützt auf berechtigte Interessen drei kumulative Bedingungen erfüllen müssen:

1. Verfolgung eines berechtigten Interesses durch den Verantwortlichen oder einen Dritten. **[➔ Wichtig ist zunächst, dass nur solche Interessen als berechtigt betrachtet werden können, die rechtmäßig, klar und präzise formuliert, real und gegenwärtig sind. Dies kann beispielsweise der Fall sein, wenn die betroffene Person Kund_in des Verantwortlichen ist oder in seinen Diensten steht.]**

2. Erforderlichkeit der Verarbeitung personenbezogener Daten zur Verfolgung des berechtigten Interesses. **[➔ Die Verarbeitung kann demnach nicht als erforderlich angesehen werden, wenn es angemessene, ebenso wirksame, aber weniger einschneidende Methoden zur Erreichung der verfolgten Interessen gibt. Hier gilt es auch den Grundsatz der Datenminimierung zu beachten.]**

3. Keine überwiegenden Interessen oder Grundfreiheiten und Grundrechte der betroffenen Person. **[➔ Der Verantwortliche muss also sicherstellen, dass sein berechtigtes Interesse nicht durch Interessen, Grundrechte oder Grundfreiheiten der Betroffenen dominiert wird. Bei dieser Abwägung müssen Verantwortliche die Interessen der Personen sowie ihre vernünftigen Erwartungen, die Auswirkungen der Verarbeitung und zusätzliche Schutzmaßnahmen berücksichtigen. Wir begrüßen an dieser Stelle die Aussage in den Leitlinien, dass gerade keine überwiegenden Interessen des Verantwortlichen im Vergleich zur betroffenen Person vorliegen müssen. Gleichwertige Interessen, die lediglich nicht überwogen werden, reichen hingegen aus, wie wir auch in unserem Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz" darstellen (s. auch S. 14 und 130 ff.).]**

Digitalisierung vom Boden bis in den Cloud-Himmel.

Die Leitlinien stellen über die rechtlichen Anforderungen hinaus anhand verschiedener Schritte auch anschaulich dar, wie Verantwortliche diese Bewertung in der Praxis durchführen können. Hierbei wird auf eine Reihe spezifischer Verarbeitungssituationen wie Betrugsprävention, Direktwerbung, oder Verarbeitung in Unternehmensgruppen eingegangen. Das Papier erläutert zudem die Beziehung zwischen der Rechtsgrundlage aus Art. 6 Abs. 1 Buchst. f) und verschiedenen Betroffenenrechten aus der DS-GVO. Besonders hervorzuheben ist hier die Formulierung der Leitlinien, dass die bloße Erfüllung der Informationspflichten aus den Art. 12-14 DS-GVO für sich genommen nicht ausreichend ist, um davon auszugehen, dass die betroffenen Personen deshalb eine bestimmte Verarbeitung vernünftigerweise erwarten können. Dies entspricht unserer der Ansicht, dass andererseits eine überobligatorische Erfüllung der Informationspflichten mit umfassender Beschreibung der Verarbeitungstätigkeiten und Interessenabwägung mit gesteigertem Informationsgehalt an die betroffenen Personen einen Einfluss auf den Abwägungsprozess der Interessen haben kann.

Die nun veröffentlichte Fassung der Leitlinien unterlag sechs Wochen lang bis zum 20. November 2024 der öffentlichen Konsultation. Stakeholder

wie Unternehmen, öffentliche Stellen, Privatpersonen, Verbände, etc. konnten hierbei ihre Ansichten und Anmerkungen zu dem Leitlinien-Entwurf kommunizieren. Die eingegangenen Meldungen wird der EDSA prüfen und gegebenenfalls in eine überarbeitete Version einbringen.

☛ Weitere Informationen

Leitlinien zur Verarbeitung personenbezogener Daten auf Grundlage von Art. 6 Abs. 1 Buchst. f) DS-GVO:
edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en

Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz":
www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

Am 19. Juni 2024 veröffentlichte der EDSA Leitlinien zu Art. 37 der JI-Richtlinie als Version 2.0, nachdem die erste Version die öffentliche Konsultation durchlaufen hat. Ebenfalls infolge der Überarbeitung nach der öffentlichen Konsultation erließ der EDSA am 07. Oktober 2024 außerdem Leitlinien zum technischen Anwendungsbereich von Art. 5 Abs. 3 der e-Privacy Richtlinie.

EDSA Leitlinien zu Art. 37 der JI-Richtlinie vom 19.06.2024:
edpb.europa.eu/system/files/2024-06/edpb-guidelines-202301_art_37_led_final_0_en.pdf

Leitlinien zum technischen Anwendungsbereich von Art. 5 Abs. 3 der e-Privacy Richtlinie vom 07.10.2024:
edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf

Das Arbeitsprogramm des Europäischen Datenschutzausschusses 2024–2025

Der Europäische Datenschutzausschuss (EDSA) ist ein unabhängiges europäisches Gremium und bildet die Dachorganisation, die die nationalen Datenschutzaufsichtsbehörden der Länder des Europäischen Wirtschaftsraums sowie den Europäischen Datenschutzbeauftragten (EDSB) zusammenbringt. Seine Aufgabe ist es, die einheitliche Anwendung der DS-GVO sowie der JI-Richtlinie sicherzustellen und die Zusammenarbeit zwischen den Aufsichtsbehörden zu gewährleisten. Zu den wichtigsten Instrumenten des EDSA zählen – ähnlich wie bei der DSK – Stellungnahmen, Beschlüsse und Leitlinien. Detaillierte Informationen über die Arbeit des EDSA können hier abgerufen werden: edpb.europa.eu/edpb_de

Am 8. Oktober 2024 hat der Europäische Datenschutzausschuss sein Arbeitsprogramm zur Umsetzung und Erfüllung dieser Aufgaben für (den Rest des Jahres) 2024 sowie 2025 beschlossen. Es besteht aus vier Säulen mit jeweils einer Vielzahl an Maßnahmen. Die zentralen Säulen sind:

- Verstärkte Harmonisierung und Förderung der Einhaltung der Vorschriften;
- Gemeinsame Rechtsdurchsetzung und effektive Zusammenarbeit;
- Gewährleistung des Datenschutzes mit Blick auf unterschiedliche Regulierungen;
- Globaler Dialog zum Datenschutz.

Maßnahmen der ersten Säule sind unter anderem die Erarbeitung von Leitlinien zur Anonymisierung, Pseudonymisierung, zur Interessenabwägung nach Art. 6 Abs. 1 Buchst. f) DS-GVO, den personenbezogenen Daten von Kindern und den Consent-or-pay-Modellen. Verschiedene weitere Veröffentlichungen zur Datenschutz-Zertifizierung, IT-Sicherheit sowie die regelmäßige Beratung der gesetzgebenden Gewalt auf EU-Ebene sind ebenfalls geplant.

Die zweite Säule umfasst im Wesentlichen Maßnahmen, die die Zusammenarbeit zwischen den Aufsichtsbehörden betreffen. Hier ist insbesondere die Arbeit des Coordinated Enforcement Framework (CEF) hervorzuheben. Nicht nur, weil es als flexible und koordinierte gemeinsame Maßnahme eine effektive Methode der Mitgliedsstaaten darstellt, konkrete Ergebnisse hinsichtlich eines zuvor festgelegten Themas mit Bezug zur Datenschutz-Praxis zu erzielen. Sondern aus baden-württembergischer Sicht gerade auch deshalb, weil wir im CEF 2025 die Federführung übernehmen (s. auch S. 38 ff.).

In der dritten Säule sind Themen versammelt, die sich auf die verschiedenen Digitalrechtsakte beziehen. Die KI-Verordnung, der Digital Markets Act, der Digital Services Act und weitere europäische Regulierungen haben allesamt Auswirkungen auf datenschutzrechtliche Fragen, zu denen sich der Europäische Datenschutzausschuss positionieren möchte. Hierzu sind unter anderem Leitlinien zu den verschiedenen Digitalrechtsakten geplant. Weitere geplante Leitlinien betreffen die Sammlung von Daten für das Training von generativer künstlicher Intelligenz, die Blockchain und die Nutzung von Social-Media-Plattformen durch öffentliche Einrichtungen. An einigen dieser Leitlinien werden auch wir berichterstattend tätig sein. Auf manche gehen wir in diesem Kapitel ein, wir berichteten auch in unserem vergangenen Tätigkeitsbericht darüber.

Abschließend soll in der vierten Säule der globale Austausch zu Fragen des Datenschutzes fortgeführt werden. Thema ist hierbei insbesondere, wie Datenübermittlungen in Länder, in denen die DS-GVO beziehungsweise die JI-Richtlinie nicht gelten, gestaltet werden können. Daneben soll die Zusammenarbeit mit den Datenschutzaufsichtsbehörden in diesen Ländern gestärkt werden.

Das Arbeitsprogramm spiegelt die stetige Entwicklung und große Bedeutung des Themas Datenschutz in allen Lebensbereichen wieder. Während der (technische) Fortschritt immer weiter wächst, muss die Datenschutzaufsicht das Grundrecht auf informationelle Selbstbestimmung in all diesen Bereichen weiter schützen und überwachen. Wir begrüßen deshalb vor allem den Fokus auf technische Maßnahmen, der eine der Grundlagen des neuen Arbeitsprogramms des EDSA bildet.

☛ Weitere Informationen

Das komplette Arbeitsprogramm des EDSA (englisch): edpb.europa.eu/system/files/2024-10/edpb_work_programme_2024-2025_en.pdf

39. Tätigkeitsbericht Datenschutz 2023 des LfDI BW: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf, S.13–23

Die EU wird immer und immer digitaler

Die Stabsstelle für Deutsche und Europäische Zusammenarbeit berichtet im Rahmen der Tätigkeitsberichte regelmäßig über die Neuerungen und Entwicklungen, die die europäische Digital-Strategie mit sich bringt. Für 2024 sollen zwei Aspekte neu und genauer beleuchtet werden.

Ein weiterer Rechtsakt aus der Familie des Digital-Pakets der EU: Der Data Act konkretisiert Auskunftsrecht und Datenübertragbarkeit

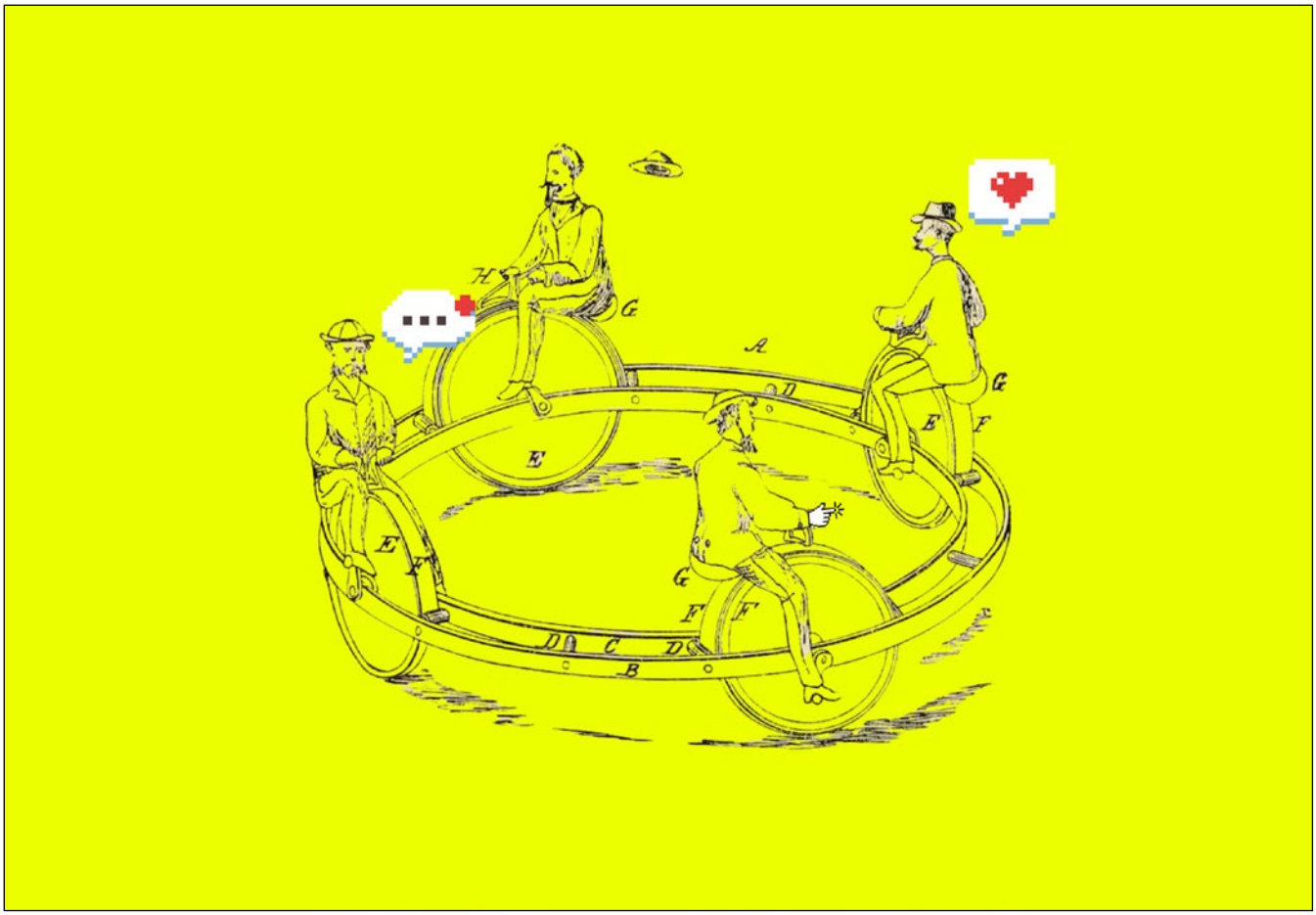
Im Januar 2024 trat der Data Act (der deutsche Begriff „Datenverordnung" wird eher selten genutzt) in Kraft. Aus Sicht des Datenschutzes ist dieser deshalb besonders interessant, weil er eine Ausformung des Auskunftsrechts nach Art. 15 DS-GVO sowie des Rechts auf Datenübertragbarkeit aus Art. 20 DS-GVO darstellt.

Aus Sicht einer Privatperson ergibt sich durch den Data Act folgende Änderung:

Vernetzte Geräte (also Geräte, die Daten produzieren und die eine Möglichkeit zum Abruf dieser Daten bieten) müssen zukünftig so ausgestaltet sein, dass den Nutzenden Zugriff auf diese – vom vernetzten Gerät erhobenen – Daten ermöglicht wird und dass diese Daten in einem nutzerfreundlichen Format bereitgestellt werden.

Wer beispielsweise zukünftig eine internetfähige Heizungssteuerung oder einen intelligenten Staubsaugerroboter erwirbt, muss beim Kauf bereits darüber aufgeklärt werden, wie die hierbei generierten Daten abgerufen werden können. Der Abruf kann beispielsweise über ein Datenkabel, eine Bluetoothverbindung oder ein Benutzerkonto beim Hersteller des Gerätes erfolgen.

Dies wirkt vielleicht auf den ersten Blick wenig aufregend, hat aber große Auswirkungen. Zunächst umfasst der Anspruch personenbezogene Daten – soweit wenig überraschend. Darüber hinaus erstreckt sich der Anspruch jedoch auch auf Daten, die das Gerät erhebt, die aber nicht unbedingt personenbezogen sein müssen. Wer also beispielswei-



Man kann sich im Internet stundenlang bewegen und auch im Kreis drehen. Die EU will mit ihren Daten- und Digitalakten Regelungen schaffen, damit die Digitalisierung nicht Selbstzweck ist, sondern den Menschen dient.

se einen Fitnesstracker gekauft hat, aber mit der App des Herstellers unzufrieden ist, könnte zukünftig neben Puls, Geschwindigkeit und Körpertemperatur auch Daten, die der Tracker über sich selbst oder die Umwelt erhebt (und die möglicherweise nicht personenbezogen sind), abrufen und in eine andere App einpflegen. Somit wird eine Nutzung dieser Daten ermöglicht, ohne zwingend auf eine bestimmte Software angewiesen zu sein.

Ebenso sieht der Data Act vor, dass die Nutzenden verlangen können, dass Daten ihres vernetzten Gerätes, die bei einem Dateninhaber (häufig der Hersteller) gespeichert sind, zu einem anderen Dritten übermittelt werden. Das übliche Beispiel ist hier ein vernetztes Auto, welches Daten zur Diagnose oder Verschleiß an den Hersteller sendet. Auf Verlangen können die Nutzenden diese Daten nun zu einer Werkstatt oder einem anderen Dritten übermitteln lassen.

Die Bedeutung des Data Act wird klar, wenn man bedenkt, wie viele Arten von vernetzten Geräten es bereits gibt bzw. es zukünftig geben wird. „Vernetzt" ist ein Gerät bereits dann, wenn es die Möglichkeit bietet, Daten auszulesen – dies kann bereits eine simple USB-Buchse sein, ein Internetzugang ist nicht unbedingt notwendig. Fitnesstracker, smarte Zahnbürsten, Heizungssteuerungen, Autos, intelligente Rasenmäher, internetfähige Bohrmaschinen, Smart TVs, Photovoltaik-Anlagen oder vernetztes Spielzeug gehören hier allesamt dazu. Die einzige Einschränkung ist, dass das Gerät nach dem 12. September 2026 „in Verkehr gebracht" wurde (im Wesentlichen bedeutet das: nach dem 12. September 2026 das erste Mal verkauft).

Zusammenfassend bringt der Data Act für Nutzende die Möglichkeit, durch den Abruf von verschiedenen (personenbezogenen und nicht-personenbezogenen) Daten noch stärker über die „eigenen"

Daten zu bestimmen. Während die existierenden Datenmengen mit jedem neuen vernetzten Gerät ansteigen, gibt der Data Act uns allen ein Mittel in die Hand, diese Daten auch für unsere eigenen Zwecke zu nutzen und formuliert damit das Recht auf Auskunft und Kopie nach Art. 15 DS-GVO weiter aus.

Die Umsetzung des Data Acts wird für uns in Zukunft eine weitere Aufgabe darstellen, denn die Datenschutzaufsichtsbehörden werden speziell mit der Überwachung der Anwendung des Data Acts beauftragt, soweit personenbezogene Daten betroffen sind. Der Data Act stellt hierbei klar, dass die Verarbeitung personenbezogener Daten im Einklang mit den Bestimmungen der DS-GVO erfolgen muss. Vor dem Hintergrund des weiten Begriffs des Personenbezugs aus Art. 4 Nr. 1 DS-GVO, der auch bei einer Identifizierbarkeit greift, dürfte der Anwendungsbereich der DS-GVO und damit die Kompetenz der Datenschutzaufsichtsbehörden in vielen Fallkonstellationen gegeben sein.

Eine praktische Herausforderung wird es sein, die Datenbestände in einem vernetzten Gerät den jeweiligen Nutzenden korrekt zuzuordnen. Werden Geräte nur von einer Person genutzt, dürfte dies unproblematisch möglich sein (Beispiel: ein Fitnesstracker wird üblicherweise nur von einer Person genutzt). Probleme kommen aber auf, wenn mehrere Personen dasselbe vernetzte Gerät nutzen. Dies kann beispielsweise bei einem Mietwagen der Fall sein. Hier hat jeder Nutzende grundsätzlich ein Recht darauf, die Daten, die während der Nutzung anfallen, abzurufen. Wenn diese Datensätze nicht klar nach Nutzenden unterschieden werden können, besteht die Gefahr, dass auch Datensätze, die andere Personen betreffen, abgerufen oder sogar zusammengeführt werden. Dies kann einen Verstoß gegen die DS-GVO darstellen, was wiederum den gesamten Katalog der aufsichtsrechtlichen Maßnahmen der Datenschutzaufsicht oder Schadenersatzforderungen eröffnet.

Daneben muss der deutsche Gesetzgeber in naher Zukunft eine zuständige Behörde zur Durchsetzung des Data Acts benennen. Aufgabe dieser Behörde wird es dann auch sein, die hier nicht behandelten Regelungen zur Datennutzung in der Wirtschaft zu zu überwachen). Ebenso müssen nationale Regelungen zur Ausgestaltung eines Sanktionsregimes nach dem Data Act selbst getroffen werden, hierfür sieht der Data Act eine Frist bis zum 12. September 2025 vor (Art. 40 Data Act). Wann eine (neue) Bundesregierung einen solchen Gesetzesentwurf vorlegen und wie die erforderliche Zusammenarbeit mit der Datenschutzaufsicht gewährleistet werden wird, bleibt abzuwarten.

Der Data Act stellt einen weiteren Rechtsakt aus dem digitalen Paket der EU dar, über das die Stabsstelle für Deutsche und Europäische Zusammenarbeit regelmäßig berichtet (zuletzt im Tätigkeitsbericht Datenschutz 2023, S. 16–21). Wie im Zusammenhang mit den anderen Rechtsakten wird auch beim Data Act eine weitere Herausforderung das Verhältnis zur DS-GVO sein. Da der Data Act selbst klarstellt, dass er keine Rechtsgrundlage für die Erhebung bzw. Generierung oder die Bereitstellung personenbezogener Daten durch den Dateninhaber darstellt, wird dieses Verhältnis für die Aufsichtsbehörden von zentraler Bedeutung sein. Das Zusammenspiel von Data Act und DS-GVO wird von der zuständigen Arbeitsgruppe des EDSA beleuchtet und voraussichtlich in Leitlinien aufgearbeitet.

☛ **Weitere Informationen**

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

Digitaler €uro – Die EZB erstattet Bericht(e)

Die Europäische Zentralbank (EZB) werkelt seit einigen Jahren an einer europäischen Digitalwährung für das Eurosystem: Der Digitale Euro als Ergänzung zum Bargeld. Finanzen sind Privatsache und gehen niemanden etwas an? Digitale Währungen und Online-Zahlungsmethoden werden im öffentlichen Diskurs immer wieder kritisch beleuchtet, insbesondere im Hinblick auf den Schutz der eigenen persönlichen Daten und finanziellen Transaktionen.

Mit dem digitalen Euro soll unter anderem Geldwäsche bekämpft werden.

Im vergangenen Jahr haben wir berichtet (siehe Tätigkeitsbericht Datenschutz 2023, Seite 20 f.), dass sich das Projekt seit November 2023 in der zweijährigen Vorbereitungsphase für die praktische Umsetzung befindet.

Die EZB verspricht mit dem Digitalen Euro mehr Privatsphäre und Datenschutz als andere digitale Zahlungsmittel – ganz nach dem Motto: „privacy by design". Ein politisches Ziel ist auch die Bekämpfung von Geldwäsche, welches durch die neue europäische Anti-Geldwäsche Behörde AMLA („Anti-Money-Laundering Authority) mit Sitz in Frankfurt verfolgt wird. Geplant ist, dass die EU-Behörde Mitte 2025 die Arbeit aufnimmt.

Parallel zur praktischen Umsetzung stellte die EU-Kommission auf gesetzgeberischer Ebene im Sommer 2023 einen Vorschlag für eine Verordnung zur Einführung des digitalen Euro (COM 2023 / 369) vor. Im nächsten Schritt müssen sich sowohl der Rat der Europäischen Union als auch das Parlament mit dem Entwurf befassen, um schließlich in die Trilogverhandlungen zu gehen. Im vergangenen Tätigkeitsbericht haben wir bereits den Vorschlag der Kommission sowie von der gemeinsamen Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten (EDSB) dazu vorgestellt.

Kommerzielle Zahlungsdienstleister sammeln eine beträchtliche Menge an personenbezogenen Daten. Der wesentliche Unterscheid hier aber sei, dass die EZB als öffentliche Institution kein Interesse daran habe, Zahlungsinformationen zu verkaufen oder für Marketingzwecke zu verwenden.

Es wird unter anderem berichtet, dass hohe Datenschutzstandards erarbeitet werden, damit digitale Zahlungen weitestgehend mit Bargeldtransaktionen vergleichbar sind. So sieht der digitale Euro eine Offline-Funktion vor, die den Nutzer_innen beim Bezahlen im Einzelhandel und zwischen Privatpersonen ein hohes Maß an Datenschutz bieten

soll, ähnlich wie beim Bargeld. Bei Offline-Zahlungen seien Transaktionsdaten nur den beteiligten Personen bekannt und würden nicht an Zahlungsdienstleister oder das Eurosystem weitergegeben. Online-Transaktionen sollen noch strengere Datenschutzstandards als derzeitige digitale Bezahlmethoden aufweisen, wobei die EZB „modernste Maßnahmen" wie Pseudonymisierung, Hashing und Verschlüsselung verwendet, um eine direkte Zuordnung zu den Beteiligten zu verhindern. Zahlungsdienstleister haben nur Zugang zu notwendigen personenbezogenen Daten zur Einhaltung der rechtlichen Vorgaben, wie etwa zur Geldwäschebekämpfung. Die Nutzung von Daten zu kommerziellen Zwecken erfordere die ausdrückliche Einwilligung der Nutzenden.

Im Dezember 2024 wurde nun der zweite Fortschrittsbericht veröffentlicht. Dieser setzt sich mit der Aktualisierung des Regelwerks für den digitalen Euro, dem Interessenbekundungsverfahren für potenzielle Anbieter, dem Austausch mit verschiedenen Interessengruppen sowie Nutzer_innenforschung und Testaktivität auseinander.

Bis Ende 2025 wird die EZB entscheiden, ob die nächste Phase der (praktischen) Vorbereitung für einen digitalen Euro eingeleitet wird. Bis dahin bleibt abzuwarten, wie der Gesetzgebungsprozess voranschreitet. Der EDSA wird die praktische und rechtliche Umsetzung weiterhin verfolgen und datenschutzrechtliche Belange prüfend im Auge behalten.

© Illustration: Y. Dwiputri

☛ Weitere Informationen

Digitaler Euro und Datenschutz: ecb.europa.eu/euro/digital_euro/features/privacy/html/index.de.html

Zeitplan: ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240411_item6erpb-planning2024.de.pdf

Erster Fortschrittsbericht der EZB vom Juni 2024: bundesbank.de/resource/blob/934690/f44afb50f4357518119d2ee507630cf0/mL/2024-06-24-fortschritt-digitaler-euro-download.pdf

Zweiter Fortschrittsbericht der EZB vom Dezember 2024: ecb.europa.eu/press/pr/date/2024/html/ecb.pr241202~d0b19e5e1b.de.html

39. Tätigkeitsbericht Datenschutz des LfDI BW 2023: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf, S. 20 f.

Frankfurt wird Sitz der neuen EU-Behörde zur Bekämpfung der Geldwäsche (AMLA): consilium.europa.eu/de/press/press-releases/2024/02/22/frankfurt-to-host-the-eus-new-anti-money-laundering-authority-amla

Vorschlag für eine Verordnung zur Einführung des digitalen Euro: eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52023PC0369

Als Teil eines Gesetzgebungspakets zur Digitalisierung im Finanzsektor und zum Zahlungsverkehr: bundesfinanzministerium.de/Content/DE/Standardartikel/Themen/Europa/Euro_auf_einen_Blick/Digitaler_Euro/digitaler-euro.html

Befassung mit dem Entwurf durch den Rat der Europäischen Union und Parlament, Ablauf: eur-lex.europa.eu/legal-content/DE/HIS/?uri=COM%3A2023%3A369%3AFIN

Der Fall Worldcoin – Europäische Kooperation zeigt wieder einmal Wirkung

Unsere Kolleg_innen vom Bayerischen Landesamt für Datenschutz (BayLDA) haben Ende 2024 als federführende Aufsichtsbehörde eine Anordnung gegen das Unternehmen Worldcoin erlassen. Die Untersuchung wurde unter Einbeziehung aller be-

troffenen Datenschutzaufsichtsbehörden in Europa durchgeführt und konnte durch diesen Austausch zu einem erfolgreichen Ergebnis geführt werden.

Das BayLDA ordnet das Unternehmen an:

- ein Löschverfahren gemäß der DS-GVO bereitzustellen;
- für bestimmte Verarbeitungsschritte eine ausdrückliche Einwilligung einzuholen;
- Datensätze zu löschen, für deren Verarbeitung keine ausreichende Rechtsgrundlage vorlag.

Worldcoin plant gegen die Entscheidung Klage zu erheben.

Das Geschäftsmodell von Worldcoin ist die weltweite Schaffung eines Identitäts- und Finanznetzwerks, das sog. „World Network". Um dieses Ziel zu erreichen, wird ein digitaler Ausweis mit Hilfe des Scans der Iris eines Menschen erstellt, die sog. „World ID". Diese dient dazu, die Nutzenden als einzigartigen Mensch zu identifizieren. Als Gegenleistung dafür erhalten die Nutzenden Kryptowährung. Das Unternehmen verarbeitet damit biometrische Daten, die gemäß Art. 9 DS-GVO besondere Kategorien personenbezogener Daten darstellen und einem besonderen Schutz unterliegen.

Bereits im April 2023 hatte das BayLDA von Amts wegen das Prüfverfahren eingeleitet. Bei mehreren anderen europäischen Datenschutzaufsichtsbehörden wurden ebenfalls Beschwerden gegen das Unternehmen erhoben.

Die spanische Datenschutzbehörde AEPD hatte im Frühjahr 2024 eine Vorsichtsmaßnahme erlassen, welche die Verarbeitung personenbezogener Daten durch das Worldcoin-Projekt in Spanien aussetzt. Diese Entscheidung erging nach Art. 66 Abs. 1 DS-GVO als Dringlichkeitsmaßnahme und beruhte auf außergewöhnlichen Umständen, die eine sofortige Einstellung der Verarbeitungstätigkeiten erforderten, um den Schutz personenbezogener Daten zu gewährleisten. Gegenstand der Beschwerde war insbesondere die Verarbeitung biometrischer Daten Minderjähriger. Das Unternehmen hatte auf Grund der Maßnahme der AEPD angekündigt, Änderungen bei der Datenverarbeitung vorzunehmen.

Neben der spanischen setzte auch die portugiesische Datenschutzbehörde CNPD zeitgleich die Verarbeitung biometrischer Daten, auch in Bezug auf Minderjährige, durch Worldcoin aus. Grundlage hierfür war ebenfalls eine große Zahl an Beschwerden sowie das hohe Risiko für die Grundrechte der Bürger_innen. Die Verhinderung (weiterer) möglicher Schäden rechtfertigte ein unverzügliches Eingreifen der Behörde.

Die Kooperation mit den anderen europäischen Aufsichtsbehörden konnte der Untersuchung der Kolleg_innen der bayerischen Aufsichtsbehörde zum erfolgreichen Abschluss verhelfen. Dieser Fall zeigt damit beispielhaft die gute Zusammenarbeit zwischen den zuständigen Behörden im Bereich der DS-GVO. Die zielführende Abstimmung untereinander dient der effektiven Durchsetzung der DS-GVO und stärkt die Rechte von betroffenen Personen in ganz Europa.

☛ Weitere Informationen

Erste Ergebnisse der Worldcoin-Untersuchung: BayLDA stärkt Betroffenenrechte:
lda.bayern.de/media/pm/pm2024_08.pdf

CNPD suspends collection of Worldcoin biometric data:
cnpd.pt/media/ocrc3lht/news_pt-dpa-suspends-collection-of-biometric-data-by-worldcoin_20240326.pdf

Worldcoin commits to stop its activity in Spain:
aepd.es/en/press-and-communication/press-releases/worldcoin-commits-to-stop-its-activity-in-spain

Irreführende Designs im Internet

Bereits in den Berichtsjahren 2023 und 2022 waren irreführende Designs (sogenannte Deceptive Design Patterns) für uns ein großes Thema. Der Umstand, dass es auch in diesem Jahr an dieser Stelle wieder einen Bericht wert ist, verdeutlicht die stetige Aktualität und Relevanz der Thematik.

FAQ zu Deceptive Design Patterns

Der EDSA hat im Jahr 2023 Leitlinien zum Umgang mit Deceptive Design Patterns erlassen. Diese Leitlinien stellen Empfehlungen und Anleitun-

Irreführende Design können dazu verleiten, in (s)einer Blase viel Zeit zu verbringen.

gen für das Design von Benutzeroberflächen auf Social-Media-Plattformen bereit. Von Deceptive Design Patterns spricht man, wenn Benutzeroberflächen insbesondere in sozialen Medien so ausgestaltet sind, dass sie Nutzende mit Hinblick auf die Verarbeitung personenbezogener Daten zu einer bestimmten Verhaltensweise – in der Regel zugunsten der verarbeitenden Social-Media-Plattform – verleiten. Dies kann etwa über verschiedene Aspekte beim Design, z. B. durch eine bestimmte Farbwahl oder die Platzierung von Inhalten, geschehen.

Die Leitlinien des EDSA untersuchen den Lebenszyklus eines Social-Media-Accounts und stellen diesen in fünf Anwendungsfällen (sog. Use Cases) dar. Besonders hilfreich sind die dort jeweils enthaltenen Beispiele für häufig zu findende Deceptive Design Patterns. Am Ende jedes Anwendungsfalles werden Empfehlungen (sog. Best Practices) zur effektiven Umsetzung der Vorgaben der DS-GVO gegeben. In Annex I der Leitlinien findet sich zudem eine Auflistung der verschiedenen Kategorien und Arten von Deceptive Design Patterns sowie die dadurch betroffenen Vorschriften der DS-GVO. Annex II der Leitlinien fasst abschließend die Best-Practice-Empfehlungen in einer Übersicht zusammen. Die Leitlinien richten sich insbesondere an Anbieter_innen sozialer Medien als Verantwortliche für die Verarbeitung von personenbezogenen Daten. Sie können – und sollen – aber auch dazu dienen, dass sich Bürger_innen informieren und sensibilisiert werden im Umgang mit ihren höchstpersönlichen Daten, indem sie ihr Bewusstsein mit Blick auf ihre Rechte und die Risiken, die durch Deceptive Design Patterns entstehen, schärfen.

Wir haben dies zum Anlass genommen und neue FAQ zu den Leitlinien zu Deceptive Design Patterns herausgegeben. Die FAQ bereiten den Text der Leitlinien auf, um ihn den Nutzer_innen sozialer Medien näher zu bringen und die verschiedenen Aspekte leichter zugänglich zu machen. Wir möchten die Bürgerschaft so darüber aufklären, worum es sich bei Deceptive Design Patterns handelt und wie ihnen begegnet werden kann. Nach einer allgemeinen Einführung in die Thematik und den Bezug zum Datenschutzrecht beantworten die FAQ in übersichtlicher Form die relevanten Fragen, die in den Leitlinien behandelt werden. Während sie die Definitionen genauer beleuchten, stellen sie vor allem die einzelnen Kategorien und Arten von Deceptive Design Patterns dar und zeigen durch die konkrete Bezugnahme auf die Beispiele aus den Leitlinien auf, in welcher Form sie in der Praxis vorkommen können. Verweise auf die Randnummern des Textes erleichtern den Leser_innen die Nachlese und Vertiefung in den Leitlinien. So sollen die FAQ die Nutzer_innen dabei unterstützen, ihre Privatsphäre auf sozialen Medien bewusst zu schützen.

Leider sind die Leitlinien des EDSA bislang nur auf englischer Sprache verfügbar. Auch diesem Umstand möchten wir durch die in deutscher Sprache verfassten FAQ begegnen. Die erfreuliche Nachricht ist, dass noch in der ersten Jahreshälfte 2025 mit der deutschen Übersetzung der Leitlinien zu rechnen ist. Als federführendem Berichterstatter der Leitlinien des EDSA freut uns dies für unseren Zuständigkeitsbereich in Baden-Württemberg ganz besonders.

GPEN Sweep – Weltweite Prüfung zu irreführenden Designs

Die oben beschriebenen Leitlinien des EDSA befassen sich lediglich mit der Verwendung von Deceptive Design Patterns auf Social-Media-Plattformen. Solche irreführenden Designs sind jedoch nicht nur dort vorzufinden, sondern können an vielen anderen Stellen vorkommen, an denen Nutzer_innen mit Produkten und Dienstleistungen in Berührung kommen, die auf Datenverarbeitungen beruhen. Hierzu gehören etwa Webseiten, Cookie-Banner, Online-Shops, Videospiele oder mobile Anwendungen (Apps) für Smartphones.

Dies haben wir im Jahr 2024 zum Anlass genommen, sich an einer weltweiten Prüfung von Webseiten auf Deceptive Design Patterns zu beteiligen, bei der 26 Datenschutzaufsichtsbehörden aus 21 Ländern und 27 Verbraucherschutzbehörden mehr als 1.000 Webseiten und Apps untersucht haben. Geprüft wurde, ob und wie auf Webseiten irreführende Designmuster eingesetzt werden, um Nutzer_innen zu einem bestimmten Verhalten zu verleiten, das es ihnen erschwert, informierte Entscheidungen über den Umgang mit ihren personenbezogenen Daten im Internet zu treffen. Das Ergebnis ist eindeutig: Von den 1000 überprüften Webseiten verwendete die Mehrheit irreführende Designmuster. Wir überprüften 17 Webseiten, von denen sogar durchweg alle irreführende Designmuster einsetzten.

Die hier beschriebenen Verfahren und Entwicklungen zeigen deutlich, dass die Nutzung von Online-Plattformen aus datenschutzrechtlicher Sicht stets aktuelle Fragestellungen mit sich bringt und eine wiederkehrende Aufgabe für uns ist und bleiben wird. Ein besonderer Aspekt liegt in der (Nicht-)Verwendung von irreführenden Designmustern bei den verantwortlichen Stellen, der aus unserer Sicht als Aufsichtsbehörde nach wie vor ein (zu) wenig beachtetes Thema ist.

☛ Weitere Informationen

38. Tätigkeitsbericht Datenschutz des LfDI BW, Täuschendes Design auf Social Media Plattformen: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2023/02/TB_38_Datenschutz-2022_V1-.pdf S. 49 f.

39. Tätigkeitsbericht Datenschutz des LfDI BW, Fazit: Globaler Blick, lokales Handeln: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf, S. 14 f f.

FAQ zu Deceptive Design Patterns: www.baden-wuerttemberg.datenschutz.de/faq-zu-deceptive-design-patterns

Weltweite Prüfung zu täuschenden Designs: www.baden-wuerttemberg.datenschutz.de/weltweite-pruefung-taeuschende-designs

Verbesserung des Datenschutzes

Sowohl GPEN als auch ICPEN, die gemeinsam an der Verbesserung des Datenschutzes und des Verbraucherschutzes für Personen auf der ganzen Welt arbeiten, haben hierzu Berichte veröffentlicht, in denen die Ergebnisse dargelegt werden.

Folgende Aspekte wurden bei der Prüfung in den Fokus genommen:

Komplexe und verwirrende Sprache: Mehr als 89% der Datenschutzinformationen sind lang oder verwenden eine komplexe Sprache.

Irreführende Benutzeroberfläche: 42% der überprüften Webseiten und Apps verwendeten eine emotional aufgeladene Sprache, um die Entscheidungen der Nutzer_innen über den Schutz ihrer personenbezogenen Daten zu beeinflussen. Rund 57% stellen die Option mit dem geringsten Datenschutz hervorgehoben und für die Nutzenden am einfachsten auszuwählende Option dar.

Belästigung: 35% der Webseiten und Apps forderten die Nutzer_innen wiederholt auf, ihre Absicht, ihr Konto zu löschen, noch einmal zu überdenken.

Versteckte Einstellungsmöglichkeiten: In fast 40% der Fälle wurden den Nutzer_innen Hindernisse in den Weg gelegt, wenn es darum ging, Entscheidungen zum Datenschutz zu treffen oder auf Datenschutzinformationen zuzugreifen, z. B. um Datenschutzeinstellungen zu finden oder ihr Konto zu löschen.

Erzwungene Maßnahmen: 9% der Webseiten und Apps zwangen die Nutzer_innen, beim Versuch, ihr Konto zu löschen, mehr persönliche Informationen preiszugeben, als sie bei der Eröffnung des Kontos angeben mussten.

privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns-reports-english-and-french

privacyenforcement.net/content/2024-gpen-sweep-deceptive-design-patterns

icpen.org/news/1360

Wir nennen es Löschung, Europa nennt es Erasure

Das Recht auf Löschung aus Art. 17 DS-GVO – oder anders gesagt: the right to erasure as per Art. 17 GDPR – ist eines der am häufigsten ausgeübten Rechte von betroffenen Personen. Die Bedeutung des in der DS-GVO nicht definierten Begriffs sowie die (technische) Umsetzung der Löschung stellt die Verantwortlichen vor Herausforderungen. Dem gehen wir nun auf den Grund.

Projekt Digitale Kehrwoche – Jetzt wird ausgemistet!

Meister K putzt blitz und blank den Datenschrank: Im Jahr 2025 wird das Thema Löschen von personenbezogenen Daten einen inhaltlichen Schwerpunkt bei uns bilden. Dabei fokussieren wir uns auf das Recht auf Löschung / Recht auf Vergessenwerden gemäß Art. 17 DS-GVO sowie das Löschen von Daten im Allgemeinen.

Besonders in Zeiten der digitalen Datenverarbeitung kommt dem Anspruch auf Löschung eine besonders wichtige Rolle zu. Betroffene Personen haben das Recht, die Löschung ihrer personenbezogenen Daten zu verlangen, wenn diese beispielsweise nicht mehr benötigt werden, unrechtmäßig verarbeitet wurden oder die Einwilligung widerrufen wurde. Daneben folgt aus der DS-GVO aber auch die Anforderung, dass verantwortliche Stellen proaktiv personenbezogen Daten löschen müssen, wenn diese im Sinne der DS-GVO nicht mehr verarbeitet werden dürfen, um auch dem Grundsatz der Datenminimierung Rech-

nung zu tragen. In diesem Zusammenhang ist die Erarbeitung eines funktionierenden Löschkonzepts für verantwortliche Stellen unabdingbar. Zudem ist es sinnvoll, Prozesse für die Löschung zu etablieren und regelmäßig zu überprüfen.

Die Stabsstelle für Deutsche und Europäische Zusammenarbeit ruft die Digitale Kehrwoche ins Leben – wir packen (digital) Besen und Kehrschaufel aus! Wir werden uns im Rahmen der Digitalen Kehrwoche mit Schulungen, Veranstaltungen sowie weiteren Aktionen und Praxishilfen für verantwortliche Stellen sowie der Bürger_innen dem Thema Löschen widmen.

Die allseits bekannte und beliebte schwäbische Kehrwoche ist die wöchentliche Pflicht zur Reinigung der gemeinschaftlichen Wohnräume sowie sonstiger bestimmter Flächen und Bereiche in und vor dem Haus. Die Jahrhunderte alte Hygienemaßnahme lässt sich nur zu gut auf das digitale Zeitalter übertragen. Ein Großteil der Daten, die wir tagtäglich bewusst und unbewusst speichern, ist Datenmüll: Dateien, Apps, Duplikate von Fotos und Videos, E-Mails, die vergessen auf Servern und elektronischen Geräten liegen. Und in den allermeisten Fällen Personenbezug haben. Diesen Datenmüll gilt es in regelmäßigem Rhythmus zu reduzieren – nicht nur um Energie und Ressourcen zu schonen, sondern auch um das Recht auf informationelle Selbstbestimmung zu gewährleisten! Regelungen zur Kehrwoche, also wer, was, wann und wie zu reinigen hat, werden in Hausordnungen festgeschrieben. Entsprechend existiert für das Löschen personenbezogener Daten in verantwortlichen Stellen idealerweise ein Löschkonzept. Heutzutage kann die Kehrwoche in Ihre Datenverarbeitungsroutinen einbezogen werden. Bitte löschen Sie Ihre Daten regelmäßig!

Koordinierte Durchsetzungsmaßnahme 2025 zum Recht auf Löschung / Recht auf Vergessenwerden

Die koordinierten Durchsetzungsmaßnahmen (Coordinated Enforcement Framework – CEF) des EDSA haben das Ziel, die Durchsetzung der DS-GVO und die Zusammenarbeit zwischen Datenschutzaufsichtsbehörden innerhalb der EU zu optimieren und dabei besonders praxisrelevante Themen in den Blick zu nehmen.

Im Jahr 2024 widmete sich das CEF des EDSA dem Auskunftsrecht nach Art. 15 DS-GVO. Der Themenvorschlag stammte vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und die Aktion wurde gemeinsam mit vielen Aufsichtsbehörden europaweit durchgeführt. Die koordinierte Aktion zum Auskunftsrecht ist die dritte Initiative im Rahmen des CEF. Frühere koor-

Der LfDI BW befasst sich im Jahr 2025 intensiv mit dem Recht auf Löschung.

dinierte Aktionen befassten sich im Jahr 2022 mit der Nutzung von Cloud-Diensten durch den öffentlichen Sektor, an der wir uns auch beteiligten, und im Jahr 2023 mit der Benennung und der Rolle von Datenschutzbeauftragten.

Beim Auskunftsrecht handelt es sich um ein enorm wichtiges Betroffenenrecht, da es den betroffenen Personen ermöglicht, zu überprüfen, ob ihre personenbezogenen Daten von Verantwortlichen gesetzeskonform verarbeitet werden. Es stellt nicht nur eines der am häufigsten ausgeübten Rechte von betroffenen Personen sowie Gegenstand zahlreicher Beschwerden bei Aufsichtsbehörden in der EU dar, sondern auch die Grundlage für die Ausübung der weiteren Betroffenenrechte der DS-GVO. Gegenstand der gemeinsamen Initiative war die Erarbeitung eines strukturierten Fragebogens zur Umsetzung des Rechts auf Auskunft in der Praxis, der in den teilnehmenden Mitgliedsstaaten koordiniert zum Einsatz kam.

Der EDSA hat im Januar 2025 seinen Abschlussbericht zum CEF 2024 veröffentlicht und berichtet, dass im Jahr 2024 insgesamt 1.185 Verantwortliche aus unterschiedlichen Branchen und Bereichen in ganz Europa befragt wurden.

Im Rahmen der koordinierten Durchsetzungsmaßnahme wurden verschiedene Herausforderungen identifiziert. Dazu zählen unter anderem die fehlende Dokumentation interner Verfahren zur Bearbeitung von Auskunftsersuchen sowie unnötige formale Anforderungen, die den Zugang für Betroffene erschweren. Der EDSA liefert in seinem Bericht konkrete Empfehlungen, um die Umsetzung des Auskunftsrechts sowohl für Verantwortliche als auch für Datenschutzaufsichtsbehörden zu verbessern. Ein zentraler Schwerpunkt liegt dabei auf der Sensibilisierung von Verantwortlichen hinsichtlich der EDSA-Leitlinien 01 / 2022 zum Auskunftsrecht und deren praktische Anwendung.

Trotz der identifizierten Probleme zeigt der Bericht auch positive Entwicklungen: Das Auskunftsrecht wird in vielen Fällen bereits gut umgesetzt. Beispiele hierfür sind benutzerfreundliche Online-Formulare oder Selbstbedienungssysteme, die es Betroffenen ermöglichen, ihr Recht schnell und unkompliziert wahrzunehmen.

Und nun wird es Zeit, die schwäbische Kehrwoche auch nach Europa zu bringen! Wir freuen uns deshalb besonders, ankündigen zu dürfen, dass sich für die vierte koordinierte Durchsetzungsmaßnahme 2025 der Vorschlag unserer Stabsstelle für Deutsche und Europäische Zusammenarbeit zur Umsetzung des Rechts auf Löschung / Rechts auf Vergessenwerden (Art. 17 DS-GVO) durchgesetzt hat und mit

Ab und zu einfach mal die Ordner durchgehen und löschen, was gelöscht werden kann.

der Mehrheit der Stimmen im EDSA angenommen wurde. Parallel zum eigenen Schwerpunktthema der Digitalen Kehrwoche in Baden-Württemberg werden wir also im kommenden Jahr die Federführung dieser europaweiten Aktion innehaben und mit mehr als 30 deutschen wie europäischen Aufsichtsbehörden gemeinsam daran arbeiten.

Das Recht auf Löschung ist eines der am häufigsten ausgeübten Rechte von betroffenen Personen und stellt die Verantwortlichen vor äußerst komplexe Prüfungen. Die Bedeutung des Begriffs „Löschung" ist in der DS-GVO nicht gesetzlich definiert und hängt angesichts des raschen digitalen Wandels vom aktuellen Stand der Technik ab.

Ziel dieser koordinierten Aktion ist es zunächst, Erkenntnisse zu gewinnen, wie Verantwortliche dieses Recht in der Praxis umsetzen. Dabei sollen die von verschiedenen Verantwortlichen etablierten Prozesse analysiert werden, um die wichtigsten Fragestellungen bei der Umsetzung des Rechts auf Löschung zu identifizieren. Die Ergebnisse sollen dazu dienen, bewährte Verfahren (best practices) zu identifizieren. Unser Ziel ist es, diese aufzubereiten und als Hilfestellung für verantwortliche Stellen bereitzustellen. Mehr dazu im Tätigkeitsbericht zum Jahr 2025 – stay tuned!

☛ Weitere Informationen

CEF 2025: EDPB selects topic for next year's Coordinated Action: edpb.europa.eu/news/news/2024/cef-2025-edpb-selects-topic-next-years-coordinated-action_de

Abschlussbericht zum CEF 2024: edpb.europa.eu/news/news/2025/cef-2024-edpb-identifies-challenges-full-implementation-right-access_en

Mehr zum CEF: edpb.europa.eu/coordinated-enforcement-framework_de

EU-weite Prüfung zur Nutzung von Cloud-Diensten durch den öffentlichen Bereich, aus dem Jahr 2022: www.baden-wuerttemberg.datenschutz.de/eu-weite-pruefung-cloud-dienste-oeffentlicher-bereich

Mehr zur schwäbischen Kehrwoche: landeskunde-baden-wuerttemberg.de/dei-schwaebische-kehrwoche#c99996

Schulungen – Wissen teilen großgeschrieben

Getreu dem Motto ‚sharing is caring – von Kolleg_innen für Kolleg_innen' ist es nach wie vor ein großes Anliegen der Stabsstelle für Deutsche und Europäische Zusammenarbeit, in regelmäßig stattfindenden Inhouse-Schulungen abteilungsübergreifend über aktuelle Entwicklungen zu informieren. Im Berichtsjahr hat die Stabsstelle für Deutsche und Europäische Zusammenarbeit insgesamt elf Inhouse-Schulungen im Bereich Datenschutz und Informationsfreiheit für das gesamte Kollegium des LfDI BW angeboten. Der Fokus lag in diesem Jahr auf den Digital-Rechtsakten der EU wie z. B. dem Digital Markets Act, AI Act oder Data Governance Act. Daneben wurden auch Schulungen zu Strafvorschriften aus dem BDSG oder dem Thema Kryptografie angeboten. Der Handel mit personenbezogenen Daten sowie das Verhältnis von Datenschutzrecht zu Archivgut waren in diesem Jahr als spezielle Veranstaltungen ebenfalls im Programm. Durch die Schulungen möchte die Stabsstelle dem gesamten Kollegium der Behörde die Möglichkeit geben, auf dem neusten Stand zu bleiben und sich intern fortzubilden. Es werden sowohl aktuelle als auch wiederkehrende Fachthemen aufgegriffen. Die Schulungen werden in hybrider Form in unserem Bildungszentrum durchgeführt.

Zudem hielten die Referent_innen der Stabsstelle für Deutsche und Europäische Zusammenarbeit wieder verschiedene Vorträge gegenüber verantwortlichen Stellen und anderen interessierten Gruppen. Der Schwerpunkt der insgesamt acht Schulungen lag im Berichtsjahr auf Fragen rund um KI und Datenschutz – mit Nuancierungen zu Ethik sowie Entwicklungen und Zusammenarbeit auf europäischer Ebene – und der Nutzung sozialer Medien durch öffentliche Stellen. Die hohe Nachfrage nach Schulungen auf diesen Gebieten spiegelt deutlich wieder, was im Jahr 2024 auch große Teile der täglichen Arbeit der Stabsstelle für Deutsche und Europäische Zusammenarbeit ausmachte.

Beteiligungen an Gesetzen und Verordnungen

Nach Art. 57 Abs. 1 Buchst. c) DS-GVO ist es Aufgabe der Datenschutzaufsichtsbehörden, das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung zu beraten. Diese Beratung ist wichtiger Baustein im Grundrechtsschutz, damit insbesondere in grundrechtssensiblen Bereichen mit erheblicher Eingriffsintensität der Gesetzgeber nicht nur den verfassungsrechtlichen Vorgaben (Wesentlichkeitstheorie, Übermaßverbot), sondern auch den europarechtlichen Vorgaben genügt. Soweit nämlich die DS-GVO Öffnungsklauseln für den nationalen Gesetzgeber enthält, verlangt sie von diesem „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" (Art. 9 Abs. 2 DS-GVO), „Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung" (Art. 6 Abs. 3 DS-GVO) oder „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person" (Art. 88 Abs. 2 DS-GVO). Eine frühzeitige Einbindung in den Gesetzgebungsprozess ist für uns wichtig, damit wir die Verfahren datenschutzrechtlich unterstützend begleiten können. In Baden-Württemberg ist die Beteiligung geregelt in § 26 Abs. 2 LDSG und Art. 57 Abs. 1 Buchst. c) und 36 Abs. 4 DS-GVO. Danach beteiligen die Ministerien den Landesbeauftragten rechtzeitig bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen. Insgesamt wurden wir im Jahr 2024 beteiligt bei 92 Norm- und Gesetzgebungsverfahren sowie Verordnungen und Verwaltungsvorschriften. Im Folgenden stellen wir einige Beispiele vor.

Standortdaten beim Notruf 110

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

Die Polizei Baden-Württemberg hat uns vor dem Einsatz einer neuen Technologie zur Verarbeitung von Standortdaten bei Notrufen zu Beratungszwecken eingebunden. Dabei hat sich herausgestellt: Damit diese Technologie rechtssicher eingesetzt werden kann, sollte der Gesetzgeber nachbessern – am besten bundesweit.

Befinden sich Personen in Notlagen, können sie über einen Anruf bei der 110 innerhalb kürzester Zeit Hilfe durch die Polizei erhalten. Halten sie sich beispielsweise an einem ihnen unbekannten Ort auf oder befinden sie sich in einem Zustand, in dem sie keine Angaben zu ihrem Aufenthaltsort machen können, kann die Polizei den Telefonstandort orten. Dies ist bereits jetzt zulässig, in Baden-Württemberg auf Grundlage von § 53 oder § 55 PolG, und bisher beispielsweise durch eine Funkzellenabfrage möglich. Die so erhobenen Standortdaten sind jedoch teilweise unpräzise, sodass wertvolle Zeit zur Rettung verloren gehen kann. Mit Advanced-Mobile-Location (AML) soll eine neue Möglichkeit zur Erhebung der Standortdaten von Smartphones beim Wählen der 110 verfügbar gemacht werden. Diese Standortdaten sind präziser und werden bei jeglichem Anruf bei der 110 mit einem Smartphone angeliefert. Aus datenschutzrechtlicher Sicht führt der Einsatz von AML jedoch zu Fragen, die nach unserer Auffassung vom Gesetzgeber geklärt werden müssen.

Bisher hat die Polizei Personen also orten können, wenn sie Anlass dazu hatte, von einer Notlage auszugehen und die Standortdaten benötigte, um die notwendige Hilfe zu leisten. Mit der Nutzung von AML führt nunmehr jegliches Anwählen der 110 mit einem Smartphone dazu, dass das Handy automatisch den eigenen Standort ermittelt und an einen sog. Knotenpunkt sendet. Dies geschieht unabhängig davon, ob der betroffenen Person dies bewusst ist oder sie Standortdaten auf ihrem Smartphone aktiviert hat – und unabhängig davon, ob die Daten zur Hilfeleistung tatsächlich benötigt werden. Dies allein stellt bereits eine erhebliche Änderung gegenüber den früheren Ortungsmethoden dar: Mit AML findet keine Ortung im Einzelfall mehr

statt, sondern ein Standortdatum wird automatisch verfügbar, sobald die 110 gewählt wird. Aus rechtlicher Sicht ist dafür unerheblich, dass der Zugriff auf die Daten technisch eingeschränkt ist und eine Löschung bei Nichtbedarf bereits nach einer Stunde erfolgt. Denn die vorherige Schwelle, dass die Polizei eine tatsächliche Sachlage dahingehend einschätzen musste, ob eine Notlage besteht und das Standortdatum ohne Mitwirkung der betroffenen Person erhoben werden muss, entfällt.

Darüber hinaus ist derzeit vorgesehen, die Nutzung von AML bundesweit durch einen Knotenpunkt bei der Polizei Baden-Württemberg ermöglicht wird. An diesem werden die Standortdaten aller mit einem Smartphone getätigten Notrufe angeliefert und gespeichert. Die bundesweit zuständigen Notrufstellen können diese dann bei Bedarf abrufen. Aus datenschutzrechtlicher Sicht stellt sich damit die Frage, wer Verantwortlicher für die Erhebung und Speicherung der Standortdaten ist, wenn sie am Knotenpunkt angeliefert und vorgehalten werden.

Es ist der Gesetzgeber, der Eingriffe in die Grundrechte erlaubt. Er setzt den Rahmen fest, innerhalb dessen die Exekutive ihre Befugnisse ausüben kann. Zwar gibt es gesetzliche Regelungen, die atypische und schwer vorhersehbare Konstellationen auffangen und der Exekutive einen weiten, eigenständigen Handlungsspielraum einräumen. Diese Generalklauseln, wie beispielsweise § 43 Abs. 2 PolG setzen jedoch voraus, dass der von ihnen eingeräumte Spielraum durch eine aktive Entscheidung der Exekutive genutzt wird. Denn Teil dieser Entscheidung ist die Prüfung, ob eine angestrebte Maßnahme im Einzelfall verhältnismäßig, d. h. geeignet, erforderlich und angemessen ist. Eben diese Prüfung und Entscheidung kann im Falle des Einsatzes von AML jedoch nicht getroffen werden: Da die Erhebung des Standorts automatisch und bei jeglichem Anruf erfolgt, gibt es kein Zeitfenster zur Bewertung des jeweiligen Sachverhalts.

Darüber hinaus befindet sich die Polizei bei der Erfüllung ihrer Aufgabe als Behörde der Gefahrenabwehr in einem gewissen Spannungsfeld zu ihrer Aufgabe als Strafverfolgungsbehörde. Letztere ist gesetzlich verpflichtet, bei Anhaltspunkten für eine Straftat zu ermitteln. Niemand sollte jedoch aus Sorge vor einer Strafverfolgung vom Wählen des Notrufs absehen.

Wir sind der Auffassung, dass der Gesetzgeber die automatisierte Erhebung normenklar, bestenfalls in einheitlicher Absprache mit den anderen Ländern und mit strenger Zweckbindung zur Gefahrenabwehr regeln sollte.

Übergangsweise haben wir erklärt, sich einem Pilotbetrieb des Einsatzes von AML nicht in den Weg zu stellen. Um allerdings dauerhafte Rechtssicherheit, auch für die anderen Bundesländer, zu schaffen, haben wir die gesetzliche Regelung zur automatisierten Erhebung und anschließenden Weiterverarbeitung gefordert. Darin sollte auch die Frage der Verantwortlichkeiten der Polizei Baden-Württemberg für die Daten anderer Länder normenklar geregelt sein. Der Schutz des Lebens und der körperlichen Unversehrtheit ist ein hohes Gut, hinter dem das Recht auf Informationelle Selbstbestimmung, das Recht auf Schutz von personenbezogenen Daten, zurücktreten kann. Allerdings muss der Konflikt zwischen diesen Rechtsgütern und den Interessen der Polizei an einer effektiven Aufgabenwahrnehmung im vorliegenden Fall durch den Gesetzgeber klargestellt werden. Nach Informationen des Innenministeriums wird dies derzeit in einer Arbeitsgruppe der Länder geprüft.

Der Einsatz von Advanced Mobile Location (AML) hat das Potential, hilfesuchende Personen schneller und effektiver retten zu können. Weil er allerdings mit einer automatisierten Verarbeitung von Standortdaten jeglicher, mit einem Smartphone anrufenden Person einhergeht, haben wir dazu aufgefordert, dass der Gesetzgeber tätig wird. Zum weiteren Verlauf dieses Vorhabens sind wir mit dem Innenministerium im Austausch.

Finanzierung der Schuldnerberatungsstellen

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

Vielfältige Umstände können dazu führen, dass Privatpersonen durch Zahlungsunfähigkeit in Not

geraten. Reichen Einkommen und liquides Vermögen nicht mehr aus, um die fälligen Raten zu begleichen, bieten in Baden-Württemberg rund 130 Schuldnerberatungsstellen ihre Unterstützung und Beratung an. Wir haben erreicht, dass die Förderung der Schuldnerberatungsstellen künftig ohne unmittelbare Preisgabe der Identität der Schuldner_innen gegenüber der fördernden Stelle möglich ist.

Bei der Insolvenz von Verbraucher_innen gilt es, einen Ausgleich herzustellen zwischen dem Interesse der Gläubiger_innen an einer möglichst vollständigen Befriedigung ihrer Ansprüche und dem Interesse der Verbraucherin bzw. des Verbrauchers nicht auf unabsehbare Dauer durch die Verpflichtung zur Abtragung ihrer bzw. seiner Schulden wirtschaftlich geknebelt zu sein. Das Verbraucherinsolvenzrecht sieht deswegen einige Besonderheiten vor. Zu diesen gehört u. a., dass der Verbraucher oder die Verbraucherin zunächst vor der Insolvenzantragstellung versuchen muss, sich außergerichtlich mit den Gläubiger_innen auf einen Plan zur Bereinigung seiner Schulden zu einigen. Erst wenn diese Bemühungen gescheitert sind, kann er einen Antrag auf Eröffnung eines Verbraucherinsolvenzverfahren stellen. Im Rahmen der Antragstellung muss er das Scheitern der außergerichtlichen Bereinigungsbemühungen dabei durch eine Bescheinigung einer geeigneten Person oder Stelle nachweisen, die den Verbraucher auf Grundlage einer eingehenden Prüfung der Einkommens- und Vermögensverhältnisse bei dem Einigungsversuch beraten hat (vgl. § 305 Abs. 1 Nummer 1 der Insolvenzordnung, InsO). Im anschließenden gerichtlichen Verfahren muss sodann auch das Insolvenzgericht noch einmal die Durchführung eines gerichtlichen Schuldenbereinigungsverfahrens versuchen. Sollte auch dieses scheitern, wird das gerichtliche Insolvenzverfahren durchgeführt, in dessen Folge der Verbraucher unter bestimmten Umständen erreichen kann, dass er nach einer sogenannten Wohlverhaltensperiode von seinen Altschulden befreit wird („Restschuldbefreiung“).

Damit Verbraucher auf eine dieser Weisen eine Klärung ihrer Schuldenlage erreichen können, ist es daher wichtig, dass ihnen in ausreichendem Umfang Personen oder Stellen zur Verfügung stehen, die die Schuldnerberatung im Zusammenhang mit dem vorgerichtlichen Schuldenbereinigungsversuch durchführen können und ihn ggf. auch noch bei der Antragstellung für das Verbraucherinsolvenzverfahren unterstützen. Diese Aufgaben können – neben den Angehörigen verschiedener rechtsberatender Berufe (z. B. Rechtsanwält_innen oder Steuerberater_innen) – auch Schuldnerberatungsstellen der Gemeinden oder Gemeindeverbände oder sonstiger juristischer Personen des öffentlichen Rechts, von örtlichen Verbänden der freien oder kirchlichen Wohlfahrtspflege oder von Verbraucherzentralen übernehmen.

In Baden-Württemberg erfolgt die notwendige rechtssichere Finanzierung u. a. durch Zahlung von Fallpauschalen an die Beratungsstellen. Nach § 3 des Gesetzes zur Ausführung der Insolvenzordnung (AGInsO BW). Die Aufgabe, diese Fallpauschalen auszuzahlen, war dabei schon seit 1999 per Verwaltungsvorschrift zentral dem Regierungspräsidium Tübingen zugewiesen worden, die zugleich das Verfahren zur Auszahlung regelte. Diese „Verwaltungsvorschrift des Sozialministeriums über die Gewährung von Fallpauschalen nach § 3 des Gesetzes zur Ausführung der Insolvenzordnung (VwV AGInsO)“ sollte zum 31. Dezember 2023 außer Kraft treten, so dass die Regelung mit Wirkung zum 1. Januar 2024 neu erlassen werden sollte. Hierzu bat uns das Sozialministerium gemäß Art. 36 Abs. 4 DS-GVO, § 26 Abs. 2 LDSG um Stellungnahme.

Bei Prüfung des Neuentwurfs der VwV AGInsO stellten wir fest, dass sowohl die antragstellenden Schuldnerberatungsstellen als auch das Regierungspräsidium im Rahmen der Förderung der Schuldnerberatungsstellen eine Vielzahl personenbezogener Daten verarbeiten. So ist die finanzielle Förderung der Schuldnerberatungsstellen durch das Regierungspräsidium an die Vorlage von Nachweisen geknüpft. Im Rahmen dieser Nachweise haben die Schuldnerberatungsstellen personenbezogene Daten der von der Privatinsolvenz betroffenen Personen zur Verfügung zu stellen. Anzugeben sind u. a. deren Vor- und Nachname sowie Anschrift, der Vergleich oder die Bescheinigung (über erfolglosen Ei-

nigungsversuch) mit Datum und Gläubigerzahl der verschuldeten Person. Die Verarbeitung personenbezogener Daten dient hierbei der Berechnung der Fallpauschalen, welche die Beratungsstellen erhalten. Das Regierungspräsidium hat hierbei auch zu prüfen, ob das außergerichtliche Einigungsverfahren für den Schuldner oder die Schuldnerin bereits vor Ablauf von zwei Kalenderjahren ein weiteres Mal geltend gemacht wird, was nach den rechtlichen Vorgaben die Gewährung einer Fallpauschale ausschließen würde. Rechtlich wurde die Verarbeitung personenbezogener Daten der verschuldeten Person seit Jahren auf die VwV AGInsO gestützt.

Im Rahmen der Beratungen forderten wir das Sozialministerium auf, eine gesetzliche Grundlage für die Verarbeitung von personenbezogenen Daten bei der Finanzierung der Beratungsstellen zu schaffen und das Förderverfahren an die Anforderung des geltenden Datenschutzrechts anzupassen. Problematisch war hierbei insbesondere die bislang vorgenommene Auslagerung der Verfahrensvorschriften zur Förderung in die VwV AGInsO, und zwar vor folgendem Hintergrund: Die Verarbeitung personenbezogener Daten ist nach Art. 6 Abs. 1 Buchst. e) DS-GVO u. a. dann rechtmäßig, wenn die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Gemäß Art. 6 Abs. 3 DS-GVO wird dabei die Rechtsgrundlage für die Verarbeitung gemäß Abs. 1 Buchst. e) durch Unionsrecht oder das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt, festgelegt. Nach § 4 des Landesdatenschutzgesetzes (LDSG) ist die Verarbeitung personenbezogener Daten unbeschadet sonstiger Bestimmungen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die der öffentlichen Stelle übertragen wurde, erforderlich ist. Wir gehen dabei mit der ganz herrschenden Meinung davon aus, dass die Zuständigkeit für die betreffende Aufgabe der öffentlichen Stelle durch ein Parlamentsgesetz oder zumindest Verordnungs- oder Satzungsrecht, für das wiederum eine legitimierende gesetzliche Ermächtigungsnorm vorliegen muss, zugewiesen werden muss. Darüber hinaus muss die die Aufgabe beschreibende und der öffentlichen Stelle zuweisende Norm ausreichend bestimmt und normenklar sein, um die Verarbeitung personenbezogener Daten zu rechtfertigen. Betroffenen Bürger_innen muss es möglich sein, die Rechtslage anhand der gesetzlichen Regelung zu verstehen, damit sie ihr Verhalten danach auszurichten können.

Diesen Anforderungen genügte der uns vorgelegte Regelungsentwurf nicht. Dieser Entwurf sah vor, dass das Verfahren zur Finanzierung der Beratungsstellen weiterhin auf Basis allein einer Regelung durch eine Verwaltungsvorschrift des Sozialministeriums erfolgen sollte. Eine solche Auslagerung der Regelung von Rechtsgrundlagen für die Verarbeitung personenbezogener Daten in eine Verwaltungsvorschrift (VwV AGInsO) ist jedoch nicht zulässig.

Verwaltungsvorschriften stellen Regelungen im reinen Innenverhältnis dar und sind mangels Gesetzesqualität per se bereits ungeeignet, über Art. 6 Abs. 1 Buchst. e) DS-GVO einen Rechtsgrund für die Verarbeitung personenbezogener Daten darzustellen. Anders als Rechtsverordnungen entfalten Verwaltungsvorschriften ihre Rechtswirkungen nur innerhalb der hierarchischen Verhältnisse der Verwaltung, also nur zwischen übergeordneter und nachgeordneter Behörde.

Schuldnerberatungsstellen sind jedoch nicht in jedem Fall Teil der Verwaltung, sondern oftmals auch private Stellen oder aber auch Stellen in kirchlicher Trägerschaft. Dies betrifft insbesondere die Träger der freien Wohlfahrtspflege außerhalb kommunaler Strukturen. Private Stellen der Schuldnerberatung konnten also durch die uns vorgelegte VwV-Regelung nicht erfasst werden, sondern allenfalls durch Rechtsverordnung verpflichtet werden.

Datenschutzrechtlich rieten wir dem Sozialministerium daher, zunächst eine rechtfertigende, normenklare gesetzliche Grundlage zu schaffen, beispielsweise indem, eine Verordnungsermächtigung in das Gesetz zur Ausführung der Insolvenzordnung (InsOAG BW) aufgenommen wird, die das Sozialministerium dazu ermächtigt, sowohl die Zuständigkeitsübertragung auf das Regierungspräsidium Tübingen als auch das Verfahren der

Fallpauschalen durch Rechtsverordnung zu regeln, und sodann datenschutzrelevante Regelungen in der neu zu schaffenden Rechtsverordnung getroffen werden. Das dafür erforderliche parlamentarische Gesetzgebungsverfahren war jedoch aus Zeitgründen nicht unmittelbar umsetzbar, und in der Übergangszeit wäre die Finanzierung der Schuldnerberatungsstellen gefährdet gewesen. Daher galt es, einen vorläufige Lösung zu finden, welche sicherstellte, dass das aktuell rechtswidrig ausgestaltete Verfahren zur Finanzierung der Beratungsstellen zumindest möglichst datensparsam ausgestaltet wird. Insoweit konnten wir erreichen, dass die Schuldnerberatungsstellen künftig nicht mehr Klarnamen und Anschrift des Schuldners / der Schuldnerin an das Regierungspräsidium Tübingen übermitteln, um eine Fallpauschalen zu erhalten, sondern mit einem pseudonymisierten Verfahren arbeitet. Da bei einer Pseudonymisierung der Personenbezug der betroffenen Daten nicht vollständig entfällt, konnte diese Umgestaltung des Verfahrens allerdings nicht bewirken, dass eine gesetzliche Rechtsgrundlage für die Verarbeitungsvorgänge vollständig entbehrlich geworden wäre.

Das Sozialministerium sicherte uns zu, zeitnah eine Verordnungsermächtigung zur Finanzierung der Schuldnerberatungsstellen in das AGInsO BW aufzunehmen, damit das Verfahren künftig nicht mehr innerhalb einer bloßen Verwaltungsvorschrift (VwV InsO) geregelt ist, sondern auf eine klare datenschutzrechtliche Grundlage gestützt wird.

Diese Zusage setzte das Sozialministerium binnen kürzester Zeit um: So wurde uns direkt zu Beginn des Jahres 2024 ein Regelungsentwurf des § 3 AGInsO BW übersandt. Inhaltlich wurde in § 3 AGInsO BW ein neuer Satz 2 aufgenommen, der künftig eine Ermächtigung des Sozialministeriums enthält, die Finanzierung der Schuldnerberatungsstellen durch Rechtsverordnung zu regeln. Dies ist ein erster notwendiger Schritt, um die Finanzierung der Schuldnerberatungsstellen auf datenschutzrechtlich rechtmäßigen Boden zu stellen. In einem zweiten Schritt galt es, die neue Verordnungsermächtigung zu nutzen und die Verarbeitung personenbezogener Daten durch die Schuldnerberatungsstellen und das Regierungspräsidium, die aktuell noch auf Basis einer Verwaltungsvorschrift erfolgt, in einer Verordnung zu regeln. Im Dezember 2024 übersandte uns das Sozialministerium hierzu den ersten Entwurf einer Verordnung zur Ausführung des Gesetzes zur Ausführung der Insolvenzordnung. Unsere Beratung dauert insofern aktuell noch an. Für die Übergangszeit bis zum Erlass der Verordnung und deren Inkrafttreten konnten wir indes bereits bewirken, dass das Verfahren zur Finanzierung der Schuldnerberatungsstellen datensparsamer ausgestaltet wird und die Identität der betroffenen Personen im Rahmen der Finanzierung der Schuldnerberatungsstellen gegenüber dem Regierungspräsidium nicht mehr direkt offenbart wird.

Bereits bei der Schaffung neuer Regelungs- und Gesetzesentwürfe ist der Datenschutz mitzudenken. Auch für pseudonymisierte Daten gelten die datenschutzrechtliche Vorgaben.

Neuregelung des Nachrichtendienstrechts

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

Das Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg hat 2024 einen Entwurf zu einem Gesetz zur Neuregelung des Nachrichtendienstrechts vorgelegt. Kernpunkt des Gesetzesentwurfs war ein neues Landesverfassungsschutzgesetz. Aufgrund der Entscheidungen des Bundesverfassungsgerichts (BVerfG) vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz (Az. 1 BvR 1619 / 17), vom 28. September 2022 zum Bundesverfassungsschutzgesetz (Az. 1 BvR 2354 / 13) sowie vom 9. Dezember 2022 zum Mecklenburg-Vorpommerischen Sicherheits- und Ordnungsgesetz (Az. 1 BvR 1345 / 21) war nach Einschätzung des Ministeriums eine umfassende Novellierung des Landesverfassungsschutzgesetzes unumgänglich, um die vom Bundesverfassungsgericht gemachten Vorgaben umzusetzen. Kernpunkte des Gesetzesentwurfs sind Folgende: In § 3 Abs. 1 werden die Verfassungsschutzgüter definiert. In § 7 wird der Schutz des Kernbereichs privater Lebensgestaltung und der Berufsgeheimnisträgerinnen und -träger bei der Anwendung nachrichtendienstlicher Mittel geregelt. § 8 normiert die Mitteilung

an betroffene Personen nach der Anwendung nachrichtendienstlicher Mittel neu. Es werden als neue Eingriffsschwellen „erheblich beobachtungsbedürftige“ und „gesteigert beobachtungsbedürftige“ Tätigkeiten eingeführt. § 13 regelt die Observation und den Einsatz technischer Observationsmittel. Die Ortung von Mobilfunkendgeräten, der verdeckte Einsatz technischer Mittel zur Wohnraumüberwachung und der Einsatz von Vertrauenspersonen und verdeckt arbeitenden Bediensteten werden intensiver reguliert. In §§ 18 ff. hat das Ministerium die Anforderungen für die Übermittlungen unterschiedlicher personenbezogener Daten durch das Landesamt für Verfassungsschutz an öffentliche und nichtöffentliche Stellen und in das Ausland neu gefasst. In § 25 Abs. 3 wurde ein Anspruch auf ermessensfehlerfreie Entscheidung über Auskunftsersuchen, auch wenn die anspruchsstellende Person nicht auf einen konkreten Sachverhalt hinweist und ihr Interesse an einer Auskunft darlegt, normiert. Die richterliche Vorabkontrolle wurde ausgeweitet, und der Gesetzesentwurf regelt Zuständigkeit und Verfahren. In § 42 ff. wurden Maßnahmen zur Eigensicherung des Landesamtes für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten geregelt.

In unserer Stellungnahme zur ersten Version des Gesetzesentwurfs haben wir uns auf die Vorschriften zu Datenübermittlungen durch das Landesamt für Verfassungsschutz und die Vorschriften zur Eigensicherung konzentriert.

Datenübermittlung

Bei den Vorschriften zu Datenübermittlungen haben wir teilweise höhere Anforderungen gefordert, die an die verschiedenen Datenübermittlungen gestellt werden müssen. Auch haben wir auf die aus unserer Sicht in Teilen unzureichende Bestimmtheit hingewiesen.

Maßnahmen zur „Eigensicherung“: Beschäftigten- und Besuchendendaten

Bei den Vorschriften zur Eigensicherung geht es um verdachtsunabhängige Kontrollen der Beschäftigten und Besuchenden des Landesamts für Verfassungsschutz sowie Durchsuchungen derselben, wenn tatsächliche Anhaltspunkte für sicherheitsgefährdende oder geheimdienstliche Tätigkeiten vorliegen. Zudem sollen Gegenstände, die sich im Eigensicherungsbereich befinden, sichergestellt und untersucht werden können, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass sie für eine sicherheitsgefährdende oder geheimdienstliche Tätigkeit verwendet werden oder mit solchen Tätigkeiten gewonnen worden sind, oder diese Gegenstände keiner bestimmten Person zuzuordnen sind und die Sicherstellung und Untersuchung zum Schutz vor einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit erforderlich ist. Bei Geräten der Informations- und Kommunikationstechnik soll hierbei auch das Eingreifen mit technischen Mitteln sowie das Verarbeiten der auf dem Gerät gespeicherten Informationen, einschließlich personenbezogener Daten, ermöglicht werden. Weiterhin gehören die Aufklärung und Abwehr unzulässiger Benutzung des Luftraums des Eigensicherungsbereichs des Landesamts für Verfassungsschutz mittels unbemannter Fluggeräte zu den geregelten Maßnahmen der Eigensicherung. Sie sollen durch geeignete technische Mittel gegen das unbemannte Fluggerät, dessen Steuerungseinheit oder Steuerungsverbindung erfolgen.

Wir haben Regelungen zur Konkretisierung der verfassungsrechtlichen Vorgaben hinsichtlich der Aufbewahrung bzw. Löschung der durch die Maßnahmen der Eigensicherung erhobenen Daten verlangt. Weiterhin fehlte eine Konkretisierung des vom Grundgesetz vorgegebenen Zweckbindungsgrundsatzes, da keine Vorschriften zur weiteren Verwendung der durch die Maßnahmen zur Eigensicherung gewonnenen Daten aufgenommen wurden. Zudem wurden keine Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung der betroffenen Personen bei Eigensicherungsmaßnahmen getroffen. Zu diesem Kernbereich gehört die höchstpersönliche, nichtöffentliche Kommunikation mit Personen des persönlichen Vertrauens, wie Ehe- oder Lebenspartner_innen, Geschwistern und Verwandten in gerader Linie, vor allem, wenn sie im selben Haushalt leben, Strafverteidiger_innen Ärzt_innen, Geistlichen und engen persönlichen Freund_ innen. Geschützt ist die Möglichkeit, inne-

re Vorgänge ohne Sozialbezug, wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen, und zwar ohne Angst, dass staatliche Stellen dies überwachen (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966 / 09, 1 BvR 1140 / 09 – BeckRS 2016, 44821, Rn. 121 f.). Der Gesetzgeber muss nach der Rechtsprechung des Bundesverfassungsgerichts Maßnahmen treffen, dass auf der Ebene der Datenerhebung eine unbeabsichtigte Miterfassung von Kernbereichsinformationen nach Möglichkeit ausgeschlossen wird und auf der Ebene der nachgelagerten Auswertung und Verwertung der erhobenen Daten die Folgen eines dennoch nicht vermiedenen Eindringens in den Kernbereich privater Lebensgestaltung strikt minimiert werden (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619 / 17 – BeckRS 2022, 8427, Rn. 277 und BVerfG, Beschluss vom 9. Dezember 2022 – 1 BvR 1345 / 21 – ZD 2023, 346, Rn. 109, 117). Bei dem Zugriff auf informationstechnische Systeme, wie zur Eigensicherung vorgesehen, besteht typischerweise eine besondere Kernbereichsnähe (BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619 / 17 – BeckRS 2022, 8427, Rn. 284).

Bei den verdachtsunabhängigen Kontrollen haben wir uns für eine genauere Regelung der Kontrollfrequenz, die die Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung wesentlich prägt, ausgesprochen. Ob auch vollständige oder nur stichprobenhafte Kontrollen verhältnismäßig, insbesondere angemessen, sind, lässt sich nur anhand der Größe der Gefahr von sicherheitsgefährdenden und geheimdienstlichen Tätigkeiten der Beschäftigten und Besuchenden des Landesamtes für Verfassungsschutz beurteilen. Auch bei den übrigen Maßnahmen haben wir eine genauere Regelung der Frage, welche personenbezogenen Daten unter welchen Voraussetzungen erhoben werden dürfen, angemahnt.

Zusammengefasst sollte der Gesetzgeber bei der Regelung von Datenverarbeitungen den Grundsatz der Verhältnismäßigkeit und seine Konkretisierungen durch die Rechtsprechung des Bundesverfassungsgerichts beachten. Datenverarbeitungen sollten so genau wie möglich geregelt werden. Dies ist auch außerhalb des Anwendungsbereichs des Europarechts erforderlich, da entsprechende Regelungen einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung nach Art. 1 Abs. 1 und Art. 2 Abs. 1 GG darstellen.

Im zweiten Entwurf des Gesetzesentwurfs wurden aufgrund des Beschlusses des BVerfG vom 17. Juli 2024 – 1 BvR 2133 / 22 Änderungen vorgenommen, die wir sehr begrüßen, u.a. hinsichtlich einer weiteren Konkretisierung der besonders schweren Straftat mit der Aufnahme eines Straftatenkatalogs sowie der Klarstellung der erhöhten Eingriffsschwelle bei der Zulässigkeit der längerfristigen Observationen mit technischen Mitteln bei Maßnahmen, die die Erstellung eines Bewegungsprofils ermöglichen. Ebenso wird das Aufgreifen der Eingriffsschwelle beim Einsatz verdeckter Mitarbeitenden begrüßt. Auch unsere Stellungnahme wurde aufgegriffen, so wurden beispielsweise Regelungen zur Verarbeitung personenbezogener Daten bei Maßnahmen zur Eigensicherung (insbesondere Speicherbegrenzung und Zweckbindung) sowie Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bei diesen aufgenommen. Wir werden das Gesetzgebungsverfahren weiter begleiten.

Ein neues Körperschaftsstatusgesetz

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

Wir haben uns mit dem Entwurf für ein Körperschaftsstatusgesetz befasst. Eine datenschutzrechtlich bedenkliche Hürde auf deren Weg zum öffentlich-rechtlichen Körperschaftstatus konnte verhindert werden.

Zehn Jahre nachdem Nordrhein-Westfalen im Jahr 2014 als erstes Bundesland ein eigenes Körperschaftsstatusgesetz für Religions- und Weltanschauungsgemeinschaften verabschiedet hat, beabsichtigt nun auch die baden-württembergische Landesregierung, ein solches Gesetz zu erlassen.

Mit dem geplanten Körperschaftsstatusgesetz soll festgelegt werden, unter welchen Voraussetzungen die Religions- und Weltanschauungsgemeinschaften den Status als Körperschaft des öffentlichen Rechts verliehen bekommen können, er ihnen aber auch wieder entzogen werden kann.

Dass hierbei vom Gesetzgeber im ersten Gesetzesentwurf im Rahmen des Antragsverfahrens die Vorlage eines Mitgliederverzeichnisses durch die jeweilige Religions- oder Weltanschauungsgemeinschaft verlangt wurde, das umfang- und detailreiche personenbezogene Daten ihrer Mitglieder enthält, hatten wir für nicht erforderlich und zu unbestimmt erachtet. Wie wir kurz vor Redaktionsschluss erfahren haben, wurden unsere Empfehlungen vollumfänglich aufgegriffen.

Was ist eine als Körperschaft des öffentlichen Rechts (KdöR) verfasste Religionsgemeinschaft?

Religions- und Weltanschauungsgemeinschaften haben unter bestimmten Voraussetzungen als Ausfluss der Grundrechte der Religions- und Vereinigungsfreiheit auch das Recht, sich zu einer Religionsgemeinschaft zusammenzuschließen (BVerfGE 137, 237 (309, Rn. 98)) und somit verfassungsrechtlich einen Anspruch darauf, dass ihnen die Rechte einer Körperschaft des öffentlichen Rechts verliehen werden (sog. „Körperschaftsstatus“). Öffentlich-rechtliche Religionsgesellschaften sollen eine effektive Form der gemeinsamen Religionsausübung bieten und dienen damit der Verwirklichung der Religionsfreiheit (BVerfGE, Urteil v. 19. Dezember 2000, 2 BvR 1500 / 97, Rz. 70.).

Eine als KdöR verfasste Religionsgemeinschaft ist eine Körperschaft des öffentlichen Rechts besonderen Typs („sui generis“). Sie unterscheidet sich grundlegend von den Körperschaften des öffentlichen Rechts im verwaltungs- und staatsorganisations-rechtlichen Sinn. Daher wird sie nicht Teil der Staatsverwaltung – dies wäre mit der aus Art. 140 Grundgesetz i.V.m. Art. 136 Abs. 1 und 4, Art. 137 Weimarer Reichsverfassung, Art. 4 Absätze 1 und 2, Art. 3 Absätze 3 S. 1 und Art. 33 Abs. 2 Grundgesetz folgenden Pflicht des Staates zu weltanschaulich-religiöser Neutralität unvereinbar. Als KdöR verfasste Religionsgemeinschaften erhalten mit der Verleihung dieses Status aber besondere Rechte wie beispielsweise das Recht zur Erhebung von Kirchensteuer, das Recht zur Ernennung von Kirchenbeamten und das Beurkundungsrecht. Neben den evangelischen Landeskirchen und den römisch-katholischen Bistümern haben in Baden-Württemberg viele weitere Religionsgemeinschaften wie z.B die Neuapostolische Kirche Süddeutschland einen solchen Körperschaftsstatus verliehen bekommen.

Vgl. die Übersicht bei Frag-den-Staat (Stand 3.6.2022) der insgesamt 34 Religionsgemeinschaften mit KdöR-Status in Baden-Württemberg, abrufbar unter:
fragdenstaat.de/anfrage/uebersicht-der-religions-und-weltanschauungsgemeinschaften-mit-status-als-kdoer-in-baden-wuerttemberg

Während des Gesetzgebungsverfahrens wurden wir zu dem geplanten Körperschaftsstatusgesetz im Rahmen des Beteiligungsverfahrens angehört und haben entsprechend zu dem uns vorgelegten 63-seitigen Gesetzentwurf Stellung genommen.

Aus datenschutzrechtlicher Sicht ist uns besonders die Vorschrift des § 4 Abs. 3 Nummer 6 des Entwurfs zum Körperschaftsstatusgesetz ins Auge gefallen. Diese Regelung sieht vor, dass eine Religions- oder Weltanschauungsgemeinschaft, welche die Verleihung des Körperschaftsstatus beantragt, als Nachweis dafür, dass sie die Gewähr bietet, dauerhaft zu bestehen und rechtstreu zu sein – Grundvoraussetzungen für die Verleihungen bzw. den Erhalt des Körperschaftsstatus – ein

» *nach Altersgruppen geordnetes Verzeichnis der Mitglieder zum Antragszeitpunkt sowie vor zehn und vor 20 Jahren einschließlich Angaben zu den Wohnorten und Staatsangehörigkeiten sowie eine Erklärung, inwieweit diese Personen bereits Mitglieder von anderen Religionsgemeinschaften oder Weltanschauungsgemeinschaften sind* «

beifügen muss. Es bedarf keiner großen Vorstel-

lungskraft, dass mit dieser Vorschrift im Bereich der vorbehaltslos gewährleisteten und grundgesetzlich verbürgten Religions- und Vereinigungsfreiheit (siehe auch Infokasten) eine Vielzahl von sensiblen personenbezogenen Daten gesammelt werden sollen, ja eventuell sogar zur Überprüfung der Rechtstreue der Gemeinschaft mit Sicherheitsbehörden abgeglichen werden sollen.

Diese Vorschrift ist nach unserer Datenschutzprüfung, die angesichts der knapp bemessenen Frist für eine Stellungnahme lediglich kursorisch erfolgen konnte, in mehreren Aspekten zu unbestimmt und daher vom Gesetzgeber vor Erlass zu überarbeiten.

Da es sich vorliegend um besonders sensible Daten (Art. 9 Abs. 1 DS-GVO) handelt, da aus ihnen die religiöse Überzeugung des jeweiligen Mitglieds hervorgeht, ist eine Verarbeitung dieser Daten nur aus Gründen eines erheblichen öffentlichen Interesses auf der Grundlage eines Gesetzes zulässig, „das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht" (Art. 9 Abs. 2 Buchst. g) DS-GVO). Der Gesetzesentwurf macht diesbezüglich keinerlei Ausführungen.

Zudem heißt es in der Einzelbegründung zu o. g. Vorschrift im Gesetzentwurf:
» *Mit dem Antrag sind verschiedene Dokumente einzureichen (Abs. 3). Der Umfang entspricht der gegenwärtigen, zwischen den Ländern abgestimmten Praxis und ergibt sich aus dem Zweck, Tatsachenmaterial für die Prognoseentscheidungen über Gewähr der Dauer und Rechtstreue vorliegen zu haben. Die aufgeführten Informationen sind nicht abschließend zu verstehen, sondern können Ansatz für weitere Ermittlungen des Sachverhalts sein. Der Gemeinschaft kann insbesondere aufgegeben werden, weitergehende Fragen zu beantworten oder Nachweise vorzulegen.* «

Wir haben in unserer Stellungnahme hierzu Folgendes angemerkt: Soweit die Vorschrift des § 4 Abs. 3 Nummer 6 des Entwurfs zum Körperschaftsstatusgesetz vorsieht, dass dem Mitgliederverzeichnis die Klarnamen ihrer Mitglieder beigefügt werden sowie Erklärungen, ob diese Personen bereits Mitglieder von anderen Religions- oder Weltanschauungsgemeinschaften sind, würden wegen der beinhalteten besonderen Kategorien personenbezogener Daten („religiöse oder weltanschauliche Überzeugungen") im Sinne des Art. 9 Abs. 1 DS-GVO besonders sensible Daten mit Personenbezug verarbeitet werden. Hierbei ist von einer entsprechend höheren Eingriffsintensität auszugehen und es gelten entsprechend strengere Voraussetzungen für die Zulässigkeit von deren Verarbeitung.

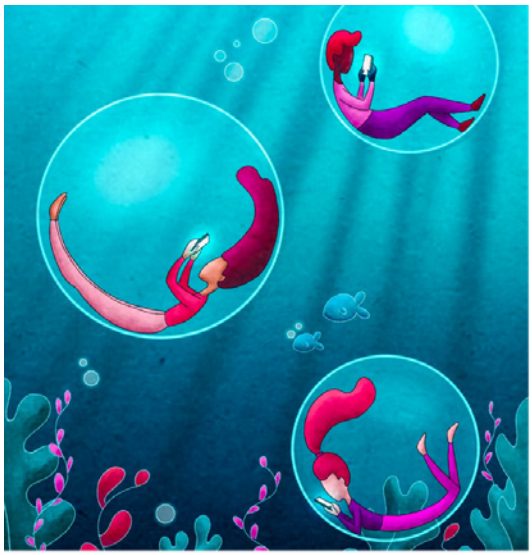
Vor diesem Hintergrund haben wir eine Überprüfung für notwendig befunden, inwieweit es für den vom Gesetzgeber angestrebten Zweck, Tatsachenmaterial für die Prognoseentscheidungen über Gewähr der Dauer und Rechtstreue von der Gemeinschaft zu erhalten, in einem ersten Verfahrensschritt nicht ausreichen würde, sich das Mitgliederverzeichnis zunächst nur mit pseudonymisierten Daten (zum Begriff der Pseudonymisierung vgl. Art. 4 Nummer 5 DS-GVO) oder anonymisierten Daten, also Daten ohne Personenbezug, vorlegen zu lassen und nur bei Zweifeln oder Nachermittlungen die Klarnamen im Nachgang anzufordern.

Sollte der Gesetzgeber jedoch tatsächlich erwägen, sich bereits in einem ersten Verfahrensschritt generell und ohne konkreten Anlass in Form des Mitgliederverzeichnisses personenbezogene Daten (besonderer Kategorien) vorlegen zu lassen, so haben wir ihm gegenüber in unserer Stellungnahme betont, dass die vorgesehene Vorschrift zu unbestimmt ist. Es müsste sich dem Wortlaut der Vorschrift vielmehr zweifelsfrei entnehmen lassen, welche konkreten Arten von personenbezogenen Daten (z. B. Name, Vorname des Gemeinschaftsmitglieds, dessen genaue Anschrift oder dessen Wohnort, die Dauer seiner Mitgliedszugehörigkeit zur Gemeinschaft, das genaue Datum des Beitritts zur Gemeinschaft, parallele Mitgliedschaft in anderer/n Gemeinschaft/en, ggf. namentliche Angabe der anderen Gemeinschaft etc.) zu übermitteln sind.

Ferner haben wir darauf aufmerksam gemacht, dass für den Fall, dass der Gesetzgeber tatsächlich beabsichtigen sollte, Klarnamen der Religions- bzw. Weltanschauungsgemeinschafts-Mitglieder zu ver-

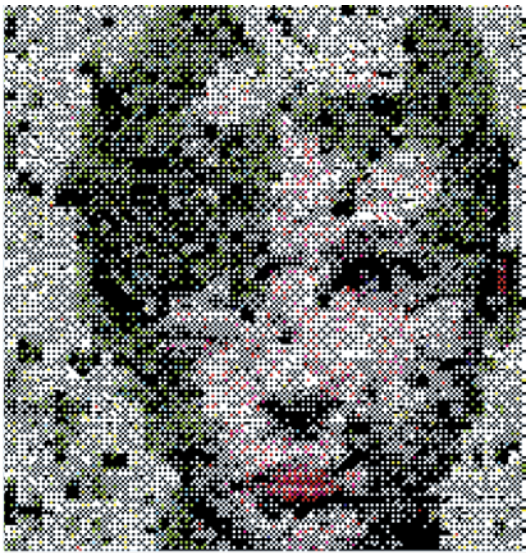
arbeiten – etwa mit der Begründung, dass andernfalls den Zweck, die wahrscheinliche „Rechtstreue“ der Gemeinschaft nicht effektiv überprüfen zu können – die Regelungen zum Körperschaftsstatusgesetz ferner zweifelsfrei erkennen lassen müssten, inwieweit sie die zuständige Behörde ermächtigen sollen, (personenbezogene) Daten aus dem Antrag oder den beigefügten Informationen beispielsweise in der Folge anderen Behörden wie z. B. dem Landesamt für Verfassungsschutz zum Datenabgleich zu übermitteln. Zudem bedürfte es auch für einen etwaigen Datenrückfluss einer Rechtsgrundlage, und zwar sowohl für die Übermittlung als auch die Erhebung.

Die obigen Vorschläge wurden dergestalt aufgegriffen, dass der Gesetzesentwurf in seiner derzeitigen Fassung nicht mehr die Vorlage von Klarnamen der Mitglieder, sondern nur noch die Vorlage eines anonymisierten Verzeichnisses der Mitglieder vorsieht. In der Gesetzesbegründung wird zudem klargestellt, dass das Gesetz weder eine Ermächtigung noch eine Verpflichtung zur Datenverarbeitung beinhaltet. Wir begrüßen die Umsetzung unserer Forderung sehr.



NEU
Häufig gestellte Fragen und Antworten zu Deceptive Design Patterns

www.baden-wuerttemberg.datenschutz.de/faq-zu-deceptive-design-patterns



VERSION 2.0
Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz

www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

Beschäftigtendatenschutz

Beratung zum Zugriff auf E-Mails, Protokolldaten und Dateiablagen

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

Das Dauerthema, unter welchen Voraussetzungen Arbeitgebende auf die Daten aus der Nutzung des dienstlichen Internetzugangs und E-Mail-Accounts sowie auf dem dienstlichen Computer abgelegte Dateien zugreifen dürfen, wurde durch eine Beratungsanfrage im Jahre 2024 relevant. Eine öffentliche Stelle in Baden-Württemberg beabsichtigte, die Nutzung der IT-Infrastruktur durch ihre Beschäftigten zu regeln, und stellte uns hierzu einige konkrete Fragen.

Bei der Frage, ob Arbeitgebende auf die Dateiablagen, die E-Mail-Accounts und die Internetprotokolldaten ihrer Beschäftigten zugreifen dürfen, sind drei Szenarien zu unterscheiden: erlaubte Privatnutzung, nicht geregelte Privatnutzung und ausdrücklich verbotene Privatnutzung. Weiterhin ist zwischen den einzelnen Datenarten (Inhalts- und Protokolldaten) zu differenzieren.

Wenn die private Nutzung gestattet ist

Bei gestatteter Privatnutzung sind im E-Mail-Postfach ggf. auch private E-Mails enthalten. Diese dürfen Arbeitgebende nicht zur Kenntnis nehmen. Ob sie nach § 3 Abs. 2 Nr. 2 und 4 TDDDG an das Fernmeldegeheimnis gebunden sind, wenn sie die private Nutzung des dienstlichen E-Mail-Accounts und Internetzugangs gestatten, ist umstritten. Wenn Arbeitgebende an das Fernmeldegeheimnis gebunden sind, dürfen sie sich oder anderen grundsätzlich nur in dem Maß Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation der Beschäftigten verschaffen, wie es für den Betrieb und die Gewährleistung der Sicherheit des Telekommunikationsnetzes und der Telekommunikationsanlagen erforderlich ist. Ausnahmen gelten bei einer Einwilligung der betroffenen Beschäftigten und einer gesetzlichen Erlaubnis. Wir vertreten die Auffassung, dass Arbeitgebende mangels Klärung der Frage bei erlaubter Privatnutzung im Zweifel von der Anwendbarkeit des Fernmeldegeheimnisses ausgehen sollen.

Ein Zugriff auf einen E-Mail-Account, dessen Privatnutzung erlaubt ist, durch Arbeitgebende kommt damit nur dann in Betracht, wenn die Beschäftigten in die entsprechenden Zugriffsrechte im Sinne von Art. 6 Abs. 1 Buchst. a) DS-GVO eingewilligt haben. Für die Wirksamkeit der Einwilligung in Eingriffe in das Fernmeldegeheimnis gelten wegen Art. 2 Buchst. f) e-Privacy-Richtlinie dieselben Anforderungen wie nach der DS-GVO. So müssen Beschäftigte vor Abgabe der Einwilligung über die wesentlichen Punkte informiert werden (vgl. EDSA, Leitlinien 05 / 2020 zur Einwilligung gemäß Verordnung 2016 / 679, 4. Mai 2020, S. 17 ff.). Problematisch ist insbesondere die Freiwilligkeit der Einwilligung. Arbeitgebende müssen Maßnahmen treffen, um das Risiko einer unfreiwilligen Einwilligung der Beschäftigten zu minimieren, etwa durch eine transparente Kopplung der Einwilligung an die Privatnutzung (nicht an die dienstliche Nutzung) und die Gewährleistung, dass den Beschäftigten bei Ablehnung der Einwilligung keine Nachteile drohen. Grundsätzlich ist eine freiwillige Einwilligung von Beschäftigten in den Zugriff auf dienstliche E-Mail-Accounts zur Ermöglichung der Privatnutzung aber möglich. Zudem müssen die Beschäftigten die Gelegenheit erhalten und verpflichtet werden, private E-Mails in einer eigenen Ablage zu speichern, auf die nicht zugegriffen wird. Hinsichtlich der Kenntnisnahme der in den privaten E-Mails enthaltenen personenbezogenen Daten dritter Personen kommt eine Einwilligung der Beschäftigten nicht als Rechtsgrundlage in Betracht. Dies gilt sowohl bezüglich der Rechtsgrundlage für die Datenverarbeitung nach Art. 6 Abs. 1 DS-GVO als auch bezüglich des Fernmeldegeheimnisses in Bezug auf die privaten Kommunikationspartner der Beschäftigten. Hier kann allerdings davon ausgegangen werden, dass eine Person, die mit einer erkennbar dienstlichen E-Mail-Adresse kommuniziert, damit rechnet, dass ggf. eine Kenntnisnahme durch andere Personen des Unternehmens / der Behörde als die

konkreten Kommunikationspartner_innen erfolgt. Damit ist die Schutzbedürftigkeit dieser Person reduziert, insbesondere wenn eine Kenntnisnahme ihrer Kommunikationsdaten bestimmungsgemäß sowieso nicht erfolgt, da nicht auf private E-Mails zugegriffen wird, und Arbeitgebende rücken der Rolle von Kommunikationspartner_innen näher. Dies rechtfertigt es, davon auszugehen, dass das Fernmeldegeheimnis nicht gegenüber privaten Kommunikationspartner_innen der Beschäftigten gilt. Soweit bekannt, erging zu dieser Problemstellung bisher aber keine gerichtlichen Entscheidungen, und sie wurde bisher auch nicht vertieft von der wissenschaftlichen oder rechtsberatenden Literatur aufgegriffen.

Wenn die Protokolldaten über die Internet- und E-Mail-Nutzung dem Fernmeldegeheimnis unterliegen, ist Arbeitgebenden ein Zugriff grundsätzlich nur mit Einwilligung der betroffenen Beschäftigten erlaubt. Dies betrifft insbesondere die Daten, aus denen sich ergibt, welche Internetseiten welche Beschäftigten wann aufgerufen haben. Ausnahmen gelten allerdings, wie oben ausgeführt, zum Schutz der technischen Systeme (z. B. erforderliche Maßnahmen zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen). Weiterhin kann § 12 Abs. 4 TDDDG eine Grundlage für den Zugriff auf dem Fernmeldegeheimnis unterliegende Protokolldaten sein: Wenn tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Telekommunikationsnetzes oder Telekommunikationsdienstes vorliegen, insbesondere für eine Leistungserschleichung oder einen Betrug oder eine unzumutbare Belästigung nach § 7 des Gesetzes gegen den unlauteren Wettbewerb, darf, wer nach § 3 Abs. 2 Satz 1 TDDDG verpflichtet ist, zur Sicherung seines Entgeltanspruchs sowie zum Schutz der Endnutzenden vor der rechtswidrigen Inanspruchnahme des Telekommunikationsdienstes oder des Tele-kommunikationsnetzes Verkehrsdaten verarbeiten, die erforderlich sind, um die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes oder Telekommunikationsdienstes aufzudecken und zu unterbinden.

Private Dateiablagen auf den Computern der Beschäftigten unterliegen unstreitig nicht dem Fernmeldegeheimnis. Hier geht es nicht mehr um Kommunikationsdaten, da ein etwaiger Kommunikationsvorgang schon abgeschlossen ist und die auf der Ablage abgelegten E-Mails und sonstigen Daten sich im Herrschaftsbereich der Empfänger_innen / Beschäftigten befinden. Ein Zugriff auf die in der privaten Ablage abgelegten personenbezogenen Dateien ist allerdings grundsätzlich unzulässig. Sollte ein Zugriff auf einzelne in der privaten Ablage abgelegte Dateien zur Aufklärung und Behebung eines konkreten IT-Sicherheitsvorfalls erforderlich sein, könnte dies unter die Aufgabenerfüllung einer öffentlichen Stelle fallen, zu der zumindest nach einer Auffassung auch die Gewährleistung der IT-Sicherheit gehört und die nach Art. 6 Abs. 1 Buchst. e) DS-GVO i.V.m. § 4 LDSG oder spezielleren Normen ein zulässiger Grund für eine Datenverarbeitung sein kann. Für private Stellen wäre Art. 6 Abs. 1 Buchst. f) DS-GVO relevant. Weiterhin könnte ein Zugriff auf die privaten Dateien bei einem IT-Sicherheitsvorfall erforderlich sei, um die dem Verantwortlichen im Zusammenhang mit einer Datenpanne auferlegten Pflichten nach Art. 33 und 34 DS-GVO (Dokumentation und Meldung der Datenpanne sowie ggf. Information der betroffenen Personen) zu erfüllen. Dann wäre dies nach Art. 6 Abs. 1 Buchst. c) DS-GVO i.V.m. den genannten Normen zulässig. Die privaten Ablagen mit privaten und persönlichen E-Mails und sonstigen Dateien sind durch die_den Beschäftigten selbst bei Ausscheiden aus dem Dienstverhältnis zu löschen.

Wenn die private Nutzung untersagt ist

Ist die Privatnutzung von E-Mail-Account und Internetzugang untersagt, ist das Fernmeldegeheimnis unstreitig nicht anwendbar. Die Rechtmäßigkeit des Zugriffs auf die personenbezogenen Daten richtet sich nach der DS-GVO und für öffentliche Stellen nach dem LDSG. Bei einem Verbot der Privatnutzung dürfen Arbeitgebende davon ausgehen, dass sich nur geschäftliche E-Mails in dem Postfach befinden. Hier haben sie grundsätzlich das Recht auf Kenntnisnahme dieser geschäftlichen E-Mails nach Art. 6 Abs. 1 Buchst. e) DS-GVO i.V.m. § 15 Abs. 1 Satz 1 LDSG zur Durchführung des Beschäftigungsverhältnisses und nach Art. 6 Abs. 1 Buchst. e) DS-GVO

Beim Beschäftigtendatenschutz sollte man sich nicht verheddern.

i.V.m. § 4 LDSG bzw. speziellerer Normen zur Aufgabenerfüllung. Für nichtöffentliche Stellen wäre Art. 6 Abs. 1 Buchst. b) (Durchführung des Arbeitsvertrags) und f) (berechtigtes Interesse) einschlägig. Für Zugriffe auf den E-Mail-Account ist jedoch trotzdem ein dienstliches Interesse erforderlich, z. B. Ausübung des Direktions- und Weisungsrechts hinsichtlich der Bearbeitung einer Angelegenheit, Sicherstellung der Vertretung bei Abwesenheit des Beschäftigten, stichprobenartige oder anlassbezogene Kontrolle der Einhaltung des Verbots der Privatnutzung oder sonstiger Pflichten, Leistungskontrollen. Es wäre auch zu erwägen, ob der verfolgte Zweck nicht auch dadurch erreicht werden kann, dass die Beschäftigten verpflichtet werden, die dienstlichen E-Mails selbst vorzulegen bzw. weiterzuleiten. Nur wenn dies nicht möglich ist (z. B. bei Abwesenheit oder nach Beendigung des Beschäftigungsverhältnisses), kann der Zugriff auf den E-Mail-Account durch Arbeitgebende als zur Durchführung des Beschäftigungsverhältnisses nach Art. 6 Abs. 1 Buchst. e) DS-GVO i.V.m. § 15 Abs. 1 Satz 1 LDSG bzw. Art. 6 Abs. 1 Buchst. b) DS-GVO erforderlich angesehen werden. Die Beschäftigten sind vorher zu informieren, aus welchen Gründen Zugriffe stattfinden können. Sollte sich im E-Mail-Account trotzdem unerlaubt eine erkennbar private E-Mail befinden, darf diese nicht zur Kenntnis genommen werden. Eine Kenntnisnahme wäre abzubrechen, sobald der private Charakter erkennbar wird, die_ der betroffene Beschäftigte wäre zur Löschung aufzufordern.

Die Protokolldaten über die E-Mail- und Internetnutzung dürfen bei untersagter Privatnutzung ebenfalls verarbeitet werden, wenn dies zur Durchführung des Beschäftigungsverhältnisses erforderlich ist, z. B. stichprobenartige oder anlassbezogene Kontrollen der Einhaltung des Verbots der Privatnutzung. Außerdem können öffentliche Stellen des

Landes nach § 5 Abs. 1 Satz 1 und 2 CSG Protokolldaten, die beim Betrieb von Kommunikationstechnik des Landes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Landes oder von Angriffen auf die Cybersicherheit des Landes erforderlich ist, und die an den Schnittstellen der Kommunikationstechnik des Landes anfallenden Daten können erhoben und automatisiert ausgewertet werden, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist. Der Umfang und die Zulässigkeit der Protokollierung und Auswertung der Internetnutzung der Beschäftigten sollte in einer Betriebs- oder Dienstvereinbarung bzw. in den individuellen Arbeitsverträgen oder in einer Richtlinie geregelt werden.

Wenn die private Nutzung nicht ausdrücklich geregelt ist

Wird die private Nutzung des dienstlichen E-Mail-Accounts und Internetzugangs nicht ausdrücklich geregelt, ist diese grundsätzlich untersagt. Die Beschäftigten haben kein Recht, dienstliche Dateiablagen, E-Mail-Postfächer und Internetzugänge für private Zwecke zu nutzen. Allerdings wird vertreten, dass eine bewusste Duldung der privaten Computer-, E-Mail- bzw. Internetnutzung durch Arbeitgebende dazu führen kann, dass diese nach den Grundsätzen über die betriebliche Übung gestattet wird. Zu der Frage, ob eine betriebliche Übung auch dadurch entstehen kann, dass Arbeitgebende bei einem bestehenden Verbot bzw. nicht geregelter Privatnutzung nicht ausreichend kontrollieren, ob die Beschäftigten den dienstlichen Internetzugang und den dienstlichen E-Mail-Account privat nutzen, gehen die Meinungen auseinander. Es wird vertreten, dass bei nicht geregelter Privatnutzung und selbst bei einem ausdrücklichen Verbot der privaten Nutzung eine betriebliche Übung entstehen kann, wenn nicht auf verbotene Privatnutzung kontrolliert wird (Barton NZA 2006, 460,461; Brink / Wirtz ArbRAktuell 2016, 255, 255). Eine andere Auffassung geht davon aus, dass eine betriebliche Übung voraussetzt, dass Arbeitgebende, konkret erklärungsbevollmächtigte Personen, eindeutige Kenntnisse von der Privatnutzung haben (DSK, Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Januar 2016, S. 4; LAG Berlin-Brandenburg, Urt. v. 14. Januar 2016 – 5 Sa 657 / 15 – BeckRS 2016, 67048, Rn. 85; Müller öAT 2020, 26, 27). Nur dann könne aus einem fehlenden Einschreiten gegen die Privatnutzung geschlossen werden, dass deren Duldung gewollt ist.

Letztlich ist entscheidend, ob die Beschäftigten die berechtigte Erwartung haben, dass Arbeitgebende mit einer privaten Nutzung des dienstlichen Internetzugangs und des dienstlichen E-Mail-Postfachs (in einem Rahmen, der nicht offensichtlich ihren Interessen zuwiderläuft) einverstanden sind. Ist die entsprechende Nutzung in einer Dienst- oder Betriebsvereinbarung oder einer Richtlinie untersagt, setzt dies voraus, dass Arbeitgebende zumindest konkludent zu verstehen geben, dass das Verbot nicht ernst gemeint ist, sondern beispielsweise nur eine Alibi-Funktion haben soll. Dies ist dann gegeben, wenn trotz Bekanntwerden von Verstößen keine Maßnahmen seitens der zuständigen Personen ergriffen werden. Werden lediglich Kontrollen unterlassen, so dass keine Kenntnis von der Privatnutzung vorliegt, kommt es auf den Grund hierfür an. Entscheidend ist, was aus der objektiven Sicht der Beschäftigten der Grund für das Unterbleiben von Kontrollen ist. Werden selbige deswegen unterlassen, weil es Arbeitgebenden egal ist, ob eine Privatnutzung stattfindet, und sie diese hinnehmen wollen, liegt eine betriebliche Übung vor. Werden Kontrollen jedoch aus anderen Gründen unterlassen, z. B. weil darauf vertraut wird, dass die Beschäftigten sich an das bestehende Verbot halten, wird hierdurch kein Vertrauenstatbestand geschaffen. Damit ist es bei Bestehen eines Verbots der Privatnutzung zum Vermeiden einer betrieblichen Übung ausreichend, dass entweder die Einhaltung des Verbots überhaupt irgendwie kontrolliert wird oder nicht kommuniziert bzw. der Eindruck erweckt wird, dass Kontrollen deswegen unterlassen werden, weil die Privatnutzung geduldet werden soll.

Kontrollen, ob die Regeln eingehalten werden

Eine getrennt hiervon zu betrachtende Frage ist, welcher Umfang an Kontrollen zur Überprüfung der Einhaltung des Verbots der privaten Internet-

und E-Mail-Nutzung erlaubt ist, also welche Kontrollen vorgenommen werden dürfen. Hier besteht Einigkeit, dass nur „stichprobenartige Kontrollen" zulässig sind. Was genau unter „stichprobenartige Kontrollen" zu verstehen ist, ist demgegenüber nicht geklärt. Maßgeblich ist, dass die konkrete Kontrollmaßnahme geeignet, erforderlich und angemessen ist, um einen Verstoß gegen das Verbot der Privatnutzung aufzudecken. Nur dann kann sie auf Art. 6 Abs. 1 Buchst. e) DS-GVO i.V.m. § 15 Abs. 1 Satz 1 LDSG bzw. Art. 6 Abs. 1 Buchst. b) DS-GVO gestützt werden. Es darf nicht auf personenbezogene Daten zugegriffen werden, die nicht für die Feststellung benötigt werden, ob eine private Nutzung des Internetzugangs / E-Mail-Accounts vorliegt. Beispielsweise ist kein Zugriff auf den Inhalt der E-Mails erforderlich, wenn eine Privatnutzung auch durch Auswertung der Protokolldaten feststellbar ist. Soweit eine nicht personenbezogene Auswertung der Protokolldaten zur Feststellung von Privatnutzung möglich und ausreichend ist, darf ein Personenbezug erst hergestellt werden, wenn sich ein Verdacht auf unerlaubte Privatnutzung ergeben hat. Zur Kontrolle einer privaten Internetnutzung dürfen nur Adressen und Titel der aufgerufenen Seiten und der Zeitpunkt des Aufrufs verarbeitet werden (BAG, Urteil vom 27. Juli 2017 – 2 AZR 681 / 16 – NZA 2017, 1327, Rn. 31 ff.).

Zur Beurteilung der Angemessenheit ist eine Abwägung der entgegenstehenden Interessen vorzunehmen. Bei verdachtsunabhängigen Kontrollen ist zu berücksichtigen, dass die Beschäftigten keinen Anlass zu diesen gegeben haben. Weiterhin kann von einer Kontrolle, welche Internetseiten Beschäftigte aufgerufen und mit wem sie E-Mails ausgetauscht haben, ein erheblicher Überwachungsdruck ausgehen, wenn sie zu häufig stattfindet. Hinsichtlich der Häufigkeit der Kontrollen und des Ausmaßes der dabei untersuchten Protokolldaten gibt es unserer Kenntnis nach keine konkreten Vorgaben aus Literatur oder Rechtsprechung. Wir halten aber einen Umfang von 1% für ausreichend, um dem Interesse der Arbeitgeber an einer wirksamen Kontrolle des Verbots der Privatnutzung unter Berücksichtigung der Interessen der Beschäftigten zu genügen. Damit kann dieser Anteil der in einem Jahr anfallenden Protokolldaten (Datum und Uhrzeit des Aufrufs der Internetseiten / des Mailversands, genutzte externe E-Mail-Domänen, aufgerufene URLs und übertragene Datenmengen) auf deutlich über dem üblichen Nutzungsverhalten liegende, auffällige Häufungen im Kommunikationsverhalten und einen extensiven Anstieg von Übertragungsvolumina bzw. besonders hohen Übertragungsvolumina bestimmter Internet- oder externen E-Mail-Domänen untersucht werden. Außerdem dürfen Arbeitgebende diesen Anteil an Protokolldaten auf URLs von häufig privat genutzten / dienstlich nicht benötigten Webseiten (z. B. Browser-Spiele, Urlaub, Chatten, Hobbies, Social Media, Streaming-Services) bzw. entsprechende E-Mail-Adressen als Kommunikationspartner_innen abgleichen. Bei einem Treffer dürfen die Daten dann mitarbeitendenbezogen weiter ausgewertet werden. Rhythmus sowie Umfang der Kontrolle sollten im Vorfeld festgelegt und die Beschäftigten hierüber informiert werden.

Soll bei einer erlaubten Privatnutzung die Einhaltung der Nutzungsbedingungen kontrolliert werden, ist zu beachten, dass hier verdachtsunabhängige Kontrollen nur mit Einwilligung der Beschäftigten zulässig sind. Diese Einwilligung muss freiwillig erfolgen und die Beschäftigten müssen informiert werden, in welche Kontrollmaßnahmen sie einwilligen. Weiterhin muss die Kontrollmaßnahme geeignet, erforderlich und angemessen sein, um die Einhaltung der Nutzungsbedingungen zu kontrollieren. Z. B. darf der oben genannte Anteil der Protokolldaten des Internetverkehrs mit Einwilligung der betroffenen Beschäftigten mit den URL verbotener Webseiten abgeglichen und auf Hinweise auf das erlaubte Maß übersteigende bzw. gegen sonstige Nutzungsbedingungen verstoßende Privatnutzung von Internet und E-Mail-Zugang untersucht werden.

Solange die Frage der Anwendbarkeit des Fernmeldegeheimnisses nicht abschließend geklärt ist, raten wir Arbeitgebenden davon ab, die private Nutzung des dienstlichen E-Mail-Postfachs (im Gegensatz zur privaten Internetnutzung) zu gestatten. Private Mails können auch bei einem entsprechenden Verbot weiterhin vom Dienstrechner, aber über den privaten E-Mail-Account verschickt werden. Wird die private Nutzung des Internetzugangs gestattet, ist eine Einwilligung der Beschäftigten erforderlich,

wenn Zugriffe auf Protokolldaten zu anderen Zwecken als zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsnetz und Telekommunikationsanlagen und nicht bei tatsächlichen Anhaltspunkten für einen Missbrauch der betrieblichen Kommunikationsmittel erfolgt. Arbeitgebende, die die private Nutzung des dienstlichen E-Mail-Accounts und Internetzugangs nicht erlauben möchten, sollten sich hierzu nicht in Widerspruch setzen, indem sie bei den Beschäftigten den Eindruck erwecken, diese zu dulden. Sie sollten bei bekanntgewordenen Fällen einer Privatnutzung Maßnahmen ergreifen und auch sonst nicht den Anschein erwecken, diese hinnehmen zu wollen.

Zusammengefasst sind bei der Regelung der Privatnutzung von E-Mail-Postfächern und Internetzugängen die datenschutzrechtlichen Voraussetzungen zu beachten. In der Beratung haben wir die öffentliche Stelle auf diese hingewiesen.

☛ **Weitere Informationen**

Orientierungshilfe der Datenschutzaufsichtsbehörden zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz, Januar 2016
datenschutzkonferenz-online.de/media/oh/201601_oh_email_und_internetdienste.pdf

Verwendung privater Telefonnummern und E-Mail-Adressen für die Kommunikation bei IT-Notfällen

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

Eine häufige Frage von Beschäftigungsgebenden ist, zu welchen Zwecken private Kontaktdaten verwendet werden dürfen.

Uns erreichte die Beratungsanfrage eines Unternehmens, das die bei ihm gespeicherten privaten Telefonnummern und E-Mail-Adresse der Beschäftigten für Zwecke der Notfallkommunikation verarbeiten wollte. Diese wurden ursprünglich erhoben und verarbeitet, um durch die Führungskraft Beschäftigte bei ungeklärter Abwesenheit erreichen zu können. Nun sollten sie genutzt werden, um bei Ausfällen oder Manipulationen der Technik durch Dritte die betriebliche Kommunikation aufrechtzuerhalten. Dies wurde auf Art. 6 Abs. 1 Buchst. f) DS-GVO gestützt. Danach ist die Verarbeitung personenbezogener Daten rechtmäßig, wenn sie 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. Zudem liege nach Einschätzung des Anfragenden zwar eine zweckändernde Verarbeitung vor, da die Telefonnummern und E-Mail-Adressen für einen anderen Zweck verarbeitet werden sollten, als wofür sie ursprünglich erhoben wurden. Diese Zweckänderung sei aber nach Art. 6 Abs. 4 DS-GVO mit dem ursprünglichen Erhebungszweck vereinbar.

Zum Zweck der Kontaktaufnahme erhobene Daten

Generell dürfen nach Art. 6 Abs. 1 Buchst. b) DS-GVO personenbezogene Daten der Beschäftigten verarbeitet werden, wenn dies zur Durchführung des Arbeitsvertrages mit ihnen erforderlich, also verhältnismäßig ist. Beschäftigte unter ihrer privaten E-Mail-Adresse oder Telefonnummer zu kontaktieren kann geeignet sein, um einem IT-Sicherheitsvorfall oder sonstigem Notfall schnell begegnen zu können. Hierbei dürfen jedoch nur die Beschäftigten kontaktiert werden, die tatsächlich informiert werden müssen. Welche Beschäftigten bei einem IT-Sicherheitsvorfall oder sonstigen Notfall erreicht werden müssen, um den Geschäftsbetrieb aufrechtzuerhalten, Daten zu sichern und den Schaden zu begrenzen, hängt wesentlich von den konkreten Umständen ab. Die für die Datenverarbeitung verantwortliche Stelle muss, z. B. anhand eines Geschäftsfortführungs- und eines Notfallkommunikationsplans, definieren, welche Mitarbeitenden bei welchen Krisenfällen kontaktiert werden müssen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt Behörden und Unternehmen, die gerade dabei sind, ein Notfallmanagement aufzubauen, und sich dabei am BSI-Standard 100-4 ausrichten möchten, ein Umsetzungsrahmenwerk zum Notfallmanagement zur Verfügung. Dieses beinhaltet auch ein „Notfallhandbuch“, in dem die

Aspekte „Geschäftsfortführungsplan“ und „Notfallkommunikation mit Mitarbeitenden und Externen“ enthalten sind. Bei Szenarien, die nicht in dem Plan des Verantwortlichen aufgeführt sind, wäre anhand der Umstände zu entscheiden, welche Beschäftigten benötigt werden bzw. informiert werden müssen, um den Geschäftsbetrieb aufrecht zu erhalten und den Schaden zu begrenzen. Nur bei diesen können private Kontaktdaten für den Zweck der Sicherstellung des Notbetriebs bzw. der Begrenzung des Schadens in dem einschlägigen Krisenfall verarbeitet werden. Außerdem muss für den jeweiligen Fall geklärt werden, welche privaten Kontaktdaten tatsächlich benötigt werden und wie dringend die Kontaktaufnahme ggf. ist. Wird z. B. die Handynummer gebraucht oder reicht die Festnetznummer, die E-Mail-Adresse oder die Wohnanschrift?

Die Angemessenheit der Datenverarbeitung hängt wesentlich davon ab, inwieweit die Beschäftigten damit rechnen müssen, mit den vorhandenen Kontaktdaten in ihrer Freizeit von Arbeitgebendenseite kontaktiert zu werden. Sollen sie darüber informiert werden, dass ihr Arbeitsplatz kompromittiert ist und sie die Arbeit an diesem nicht aufnehmen dürfen, ist maßgebend, inwieweit diese Information den betroffenen Beschäftigten auch gegeben werden kann, wenn sie am Arbeitsplatz eintreffen. Ist dies z. B. wegen Homeoffice nicht möglich, ist eine Kontaktaufnahme bereits in der Freizeit zulässig, und die betroffene Person muss mit ihr rechnen. Das Gleiche gilt, wenn Mitarbeitende darin eingewilligt haben, in entsprechenden Fällen unter ihrer privaten E-Mail-Adresse oder Telefonnummer kontaktiert zu werden, damit sie sich ggf. den Weg zum Arbeitsplatz ersparen. Sollen Mitarbeitende verpflichtet werden, die Arbeit aufzunehmen, um dem IT-Sicherheitsvorfall oder sonstigen Notfall zu begegnen, wäre, soweit möglich, mit Anordnung von Rufbereitschaft zu arbeiten. Dann wäre für die Beschäftigten planbar, wann sie bei einem Notfall zur Aufnahme des Dienstes verpflichtet werden können. Die Nutzung von privaten E-Mail-Adressen und Handynummern, um Beschäftigte außerhalb der regulären Arbeitszeit zu kontaktieren, kommt nur in Betracht, wenn es für Arbeitgebende keine milderen Maßnahmen gibt, um den mit der Kontaktaufnahme verfolgten Zweck zu erreichen. Eine solche kann darin bestehen, dass arbeitsvertraglich oder durch Betriebsvereinbarung Zeiten vorgegeben werden, in denen die Mitarbeitenden bei Notfällen erreichbar sein und dem Arbeitgeber zur Verfügung stehen müssen (vgl. LAG Thüringen, Urteil vom 16. Mai 2018 – 6 Sa 442 / 17 – BeckRS 2018, 14747, Rn. 48 ff.).

Bereits vorliegende Daten: Zweckänderung

Sollen bereits für andere Zwecke erhobene Beschäftigtendaten für die Notfallkommunikation verwendet werden, liegt ggf. eine zweckändernde Verarbeitung vor. Dann sind Art. 5 Abs. 1 Buchst. b) DS-GVO und Art. 6 Abs. 4 DS-GVO zu beachten. Danach ist die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem diese erhoben wurden, nur unter den folgenden Voraussetzungen zulässig: Sie kann auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der europäischen Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DS-GVO genannten Ziele darstellt, beruhen. Ist dies nicht der Fall, muss der neue Zweck mit dem Erhebungszweck vereinbar sein. Kriterien für diese Vereinbarkeit sind

- die Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung, der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und der verantwortlichen (arbeitgebenden) Stelle;
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO oder personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten gemäß Art. 10 DS-GVO verarbeitet werden;
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen;
- und das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören können.

Die Verarbeitung der privaten Kontaktdaten der Beschäftigten dient letztlich dem Zweck, mit ihnen in Kontakt treten zu können, wenn dies aus dienstlichen Gründen notwendig ist und keine andere Möglichkeit der Kontaktaufnahme zur Verfügung steht. Ob diese Situation durch eine ungeplante Abwesenheit der betroffenen Beschäftigten oder einen IT-Sicherheitsvorfall begründet ist, ist letztlich nicht entscheidend. Damit ist davon auszugehen, dass die Verarbeitung von privaten Kontaktdaten, die ursprünglich dafür erhoben wurden, um Beschäftigte bei unangekündigter Abwesenheit erreichen zu können, für die Notfallkommunikation mit dem Erhebungszweck vereinbar und damit zulässig ist. Die Beschäftigten sind über diese Weiterverarbeitung und den damit verfolgten Zweck gemäß Art. 13 Abs. 3 DS-GVO zu informieren.

Ein Unternehmen bzw. eine öffentliche Stelle sollte einen Plan aufstellen, wie die Beschäftigten bei einem Ausfall der betrieblichen Kommunikationsinfrastruktur durch einen IT-Sicherheitsvorfall oder sonstigen Notfall zu informieren sind. In diesem ist auch aufzuführen, welche Beschäftigten unverzüglich informiert werden müssen. So wird nicht nur gewährleistet, dass zügig die erforderlichen Maßnahmen zur Wiederaufnahme des Geschäftsbetriebs getroffen werden, es wird auch sichergestellt, dass die privaten Kontaktdaten der Beschäftigten nur für Kontaktaufnahmen genutzt werden, die zum Erreichen des verfolgen Zwecks erforderlich und angemessen und damit datenschutzrechtlich zulässig sind. Die Beschäftigten sind hierüber zu informieren.

☛ Weitere Informationen

BSI-Standard 100-4 (Umsetzungsrahmenwerk zum Notfallmanagement):
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-100-4-Notfallmanagement/Umsetzungsrahmenwerk-zum-Notfallmanagement-nach-BSI-Standard-100-4/umsetzungsrahmenwerk-zum-notfallmanagement-nach-bsi-standard-100-4_node.html

Einsatz von Schadsoftware-Scannern

✎ Art. 57 Abs. 1 Buchst. a) DS-GVO

Im Jahre 2024 gingen wir gleich zwei anonymen Hinweisen nach, in denen sich Beschäftigte gegen die Verarbeitung ihrer personenbezogenen Daten durch von ihrem Arbeitgeber eingesetzte Programme zum Scannen auf Schadsoftware (Malware) gewandt haben. Diese ist unzulässig, wenn es an einer datenschutzrechtlichen Grundlage fehlt, insbesondere, weil das eingesetzte Programm zur Herstellung der IT-Sicherheit nicht geeignet, erforderlich und angemessen ist. Wir haben den Verantwortlichen entsprechende Hinweise erteilt.

Betroffen war einmal eine nichtöffentliche Stelle, die ein Programm zur Analyse von Netzwerkverkehr mittels TLS (Transport Layer Security)-Inspection (u. a. Entschlüsselung des mit TLS oder – dem veralteten – SSL beim Transport verschlüsselten Internetverkehrs) und zu dem Blockieren unerwünschter Webseiten eingesetzt hat, z. B. von Webseiten, die illegal urheberrechtlich geschützte Inhalte, pornographische oder gewaltverherrlichende Inhalte anbieten. Die TLS-Verschlüsselung schützt die beim Transport über das Internet übertragenen Daten davor, ausgespäht zu werden, verhindert aber auch, dass auf Netzwerkknoten Programme die übertragenen Inhalte auf Malware untersuchen können. Die TLS-Inspection funktioniert häufig ähnlich wie ein sog. „Man-In-The-Middle"-Angriff. Sie erlaubt dem Programm, sich in den Netzwerkverkehr einzuklinken und durch zusätzlich auf dem Client des Anwenders installierte Stammzertifikate bei Unterbrechung des Netzwerkverkehrs sonst erscheinende Warnmeldungen im Browser des Anwenders zu verhindern. Auf diese Weise ist es im Ergebnis möglich, den verschlüsselten Netzwerkverkehr zu untersuchen und vor schädlichen Inhalten zu warnen. Hierbei stellen sich einige datenschutzrechtliche Fragen.

So war in einem solchen Fall Art. 6 Abs. 1 Buchst. f) DS-GVO die in Betracht kommende Rechtsgrundlage. Nach ErwG 49 DS-GVO stellt die Verarbeitung personenbezogener Daten u. a. durch Anbieter von Sicherheitstechnologien und -diensten in dem Maße ein berechtigtes Interesse der jeweiligen

Verantwortlichen dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d. h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen.

Ein berechtigtes Interesse der Verantwortlichen kann daneben auch die Vermeidung einer möglichen Haftung der Arbeitgeber für Verstöße von Beschäftigten gegen das Urheberrecht sein. Eine Verwendung der durch entsprechende Programme zur Analyse des Netzwerkverkehrs verarbeiteten Daten zur Leistungs- und Verhaltenskontrolle der Beschäftigten, ausgenommen die Aufklärung eines begründeten Verdachts auf eine Straftat oder schwerwiegende Pflichtverletzung, oder zur Nachverfolgung von Arbeitsprozessen wäre unzulässig und muss klar ausgeschlossen werden.

Art. 6 Abs. 1 Buchst. c) DS-GVO erlaubt Datenverarbeitungen, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich sind, der die Verantwortlichen unterliegen. Sofern diese als Kritische Infrastruktur gemäß KRITIS-Verordnung einzustufen sind, sind sie nach § 8a Abs. 1a BSIG verpflichtet, Systeme zur Angriffserkennung einzusetzen, die geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Ob hierin eine Pflicht liegt, durch diese Systeme personenbezogene Daten verarbeiten zu lassen, ist umstritten. Den Einsatz von Systemen der IT-Sicherheit auf Art. 6 Abs. 1 Satz 1 Buchst. c) DS-GVO in Verbindung mit Art. 32 DS-GVO zu stützen, halten wir für problematisch. Es ist zweifelhaft, ob Art. 32 DS-GVO eine rechtliche Pflicht nach Art. 6 Abs. 1 Satz 1 Buchst. c) DS-GVO begründet. Er verpflichtet die verantwortlichen Stellen nicht unmittelbar dazu, personenbezogene Daten zu verarbeiten. Die in einer Vorschrift des objektiven Rechts vorgesehene „rechtliche Verpflichtung“ muss sich zumindest nach einer

Dateien nach Viren zu scannen ist gut, dabei sollte man aber Fehler vermeiden.

Ansicht unmittelbar auf die Datenverarbeitung beziehen. Allein der Umstand, dass Verantwortliche, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten müssen, reicht hiernach nicht aus (LSG Hessen BeckRS 2020, 1442 Rn. 13).

Auf jeden Fall ist zu prüfen, ob die TLS-Inspection zum Erreichen des angestrebten Zwecks geeignet, erforderlich und angemessen ist. Eine große Bedeutung kommt hier dem Stand der Technik in der Informationssicherheit zu, wie er sich z. B. im IT-Grundschutzkompendium 2023 des BSI (Bundesamt für Sicherheit in der Informationstechnik) findet. Hierin fordert dieses als SOLL-Standardanforderung (d. h. keine Basis-Anforderung und keine MUSS-Anforderung) die temporäre Entschlüsselung von verschlüsselten Verbindungen in nicht vertrauenswürdige Netze, wie das Internet, um das Protokoll zu verifizieren und die Daten auf Schadsoftware zu prüfen (BSI, IT-Grundschutzkompendium 2023, Baustein NET.3.2 Firewall, Anforderung NET.3.2.A21 Temporäre Entschlüsselung des Datenverkehrs. Hierbei muss diese Anforderung normalerweise erfüllt werden, es kann aber Gründe geben, dies nicht zu tun. Dies muss jedoch sorgfältig abgewogen und stichhaltig begründet werden (BSI, IT-Grundschutzkompendium 2023, IT-Grundschutz – Basis für Informationssicherheit, S. 6, abrufbar s. oben). Generell sind Standard-Anforderungen für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden (BSI, IT-Grundschutzkompendium 2023, Glossar, S. 7, abrufbar s. oben). Die französische ANSSI (Agence nationale de la sécurité des systèmes d'information) empfiehlt in ihren „Recommandations de sécurité concernant l'analyse des flux HTTPS" auf S. 15 ff., HTTPS-Traffic mit streng persönlichen Seiten, wie Bankseiten, nicht zu entschlüsseln. Auch das BSI weist darauf hin, dass bei der Entschlüsselung (datenschutz-)rechtliche Rahmenbedingungen einzuhalten sind.

So ist datenschutzrechtlich durch die Verantwortlichen herauszuarbeiten, welche technischen und organisatorischen Maßnahmen zum Schutz der Rechte und Freiheiten der durch die Verarbeitung betroffenen Personen einzusetzen sind. In diesem Zusammenhang haben wir die Verantwortliche auch auf den 7. Tätigkeitsbericht des Bayerischen Landesamt für Datenschutzaufsicht, Ziffer 22.5, hingewiesen. Dieses erachtet die SSL- bzw. TLS-Inspection bei erlaubter Privatnutzung nur mit wirksamer Einwilligung der Beschäftigten für zulässig und auch ansonsten für datenschutzrechtlich schwierig. Es verweist auf Schutzlücken, die durch das Aushebeln der Verschlüsselung, insbesondere beim Einsatz eines Auftragsverarbeiters, entstehen können. Allgemein ist die Umsetzung einer datenschutzkonformen TLS-Inspection, welche die IT-Sicherheit erhöht, ohne neue Risiken zu schaffen, herausfordernd.

Der zweite Fall betraf eine öffentliche Stelle, bei der ein Programm im Einsatz war, welches auf Rechnern der Mitarbeitenden nach Schadsoftware gesucht hat. Es handelte sich um ein EDR-System (Endpoint Detection and Response), welches u. a. IoC-Scans (Indicators of Compromise) und sog. Threat Hunting im Dateisystem, im Arbeitsspeicher, in der Windows-Registry und im Eventlog betrieb. Hier war zu beachten, dass sich öffentliche Stellen im Rahmen der Erfüllung ihrer Aufgaben nicht auf Art. 6 Abs. 1 Buchst. f) DS-GVO berufen können. Ob die Gewährleistung der IT-Sicherheit zu den originären Aufgaben einer öffentlichen Stelle gehört, ist umstritten (s. Nägele / Joos DuD 2022, 578, 583, Schaller / Schild NZA 2024, 505, 510 einerseits und Frenzel, in: Paal / Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 6 DS-GVO Rn. 31 sowie Jandt, in: Hornung / Schallbruch, IT-Sicherheitsrecht, 1. Aufl. 2021, § 17 Fn. 115 andrerseits). Art. 6 Abs. 1 Buchst. e) DS-GVO erlaubt Datenverarbeitungen, die für die Wahrnehmung einer Aufgabe erforderlich sind, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die den Verantwortlichen übertragen wurde. Erwägungsgrund 49 DS-GVO bezeichnet die Verarbeitung von personenbezogenen Daten, die für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, auch durch Behörden, als berechtigtes Interesse der Verantwortlichen. Die Aufgabe zur Gewährleistung von IT-Sicherheit wurde öffentlichen Stellen des Landes Baden-Württemberg durch mehrere Normen übertragen.

§ 5 Abs. 2 Satz 1 und 2 CSG erlaubt es, die Protokolldaten, die beim Betrieb von Kommunikationstechnik des Landes anfallen, zu erheben und automatisiert auszuwerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Landes oder von Angriffen auf die Cybersicherheit des Landes erforderlich ist, und die an den Schnittstellen der Kommunikationstechnik des Landes anfallenden Daten zu erheben und automatisiert auszuwerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist. Wie „beim Betrieb von Kommunikationstechnik des Landes" zu verstehen ist, ist hierbei nicht abschließend geklärt. Kommunikationstechnik umfasst nach § 2 Abs. 6 CSG die Informationstechnik, die von einer oder mehreren öffentlichen Stellen des Landes oder im Auftrag einer oder mehrerer öffentlichen Stellen des Landes betrieben wird und der Kommunikation oder dem Datenaustausch der öffentlichen Stellen untereinander oder mit dritten Personen dient. § 5 Abs. 2 Satz 1 und 2 CSG sind ausweislich der Gesetzesbegründung primär auf die Analyse des in das Landesverwaltungsnetz eindringenden Datenverkehrs bezogen. Schadprogramme sollen bereits am Übergang vom Internet zum Landesverwaltungsnetz erkannt und abgewehrt werden (s. LT-Drs. 16 / 9490, S. 45). Eine Untersuchung der Dateien auf dem Client selbst ist von § 5 Abs. 2 CSG möglicherweise nicht erfasst. Es geht hierbei nicht um Protokolldaten über den Betrieb der Kommunikationstechnik gerade beim Datenaustausch mit anderen Stellen (Clients oder Servern). Wenn bestimmte Tatsachen den Verdacht begründen, dass personenbezogene Daten ein Schadprogramm enthalten, durch ein Schadprogramm übermittelt wurden oder sich aus ihnen Hinweise auf ein Schadprogramm ergeben können, und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen, sind nach § 5 Abs. 4 CSG auch weitere Datenverarbeitungen zulässig.

§ 3 Abs. 1 LDSG verpflichtet die öffentlichen Stellen des Landes, bei der Datenverarbeitung angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Hierzu können auch Netzwerküberwachung und Anomaliedetektion gehören (s. Nägele, in Jacobi, LDSG, 1. Aufl. 2024, § 3 S. 64).

Bestehen Anhaltspunkte, dass ein IT-Sicherheitsvorfall stattgefunden hat, sind Verantwortliche verpflichtet, den Sachverhalt zu untersuchen und aufzuklären. Nur so können sie z. B. den im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten (Datenpanne) bestehenden Pflichten nach Art. 33 ff. DS-GVO nachkommen und beurteilen, ob und wenn ja welche Maßnahmen zur Beseitigung der Gefährdung der Integrität und Vertraulichkeit der von ihnen verarbeiteten (personenbezogenen) Daten getroffen werden müssen. Die hierfür notwendigen Verarbeitungen personenbezogener Daten sind nach Art. 6 Abs. 1 Buchst. c) DS-GVO zulässig.

Wir haben der öffentlichen Stelle folgende Hinweise gegeben:

1. Vor dem Einsatz eines bestimmten Programmes sollten Alternativen erwogen und eine Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignisse erstellt werden, in der u. a. die datenschutzrechtlichen Anforderungen an entsprechende Maßnahmen beschrieben werden. Maßgeblich ist, dass das verwendete Programm zum Erreichen des mit ihm verfolgten Ziels geeignet, erforderlich und mit Blick auf die Risiken und Beeinträchtigungen der Rechte und Freiheiten der von der Maßnahme betroffenen Personen angemessen ist.

2. Das Scannen von Endgeräten auf Dateinamen, -inhalte und Windows-Registry-Einträge, ohne dass Anhaltspunkte für einen Befall mit Schadsoftware vorliegen, ist rechtlich problematisch, wenn hierbei personenbezogene Daten verarbeitet werden. Auf jeden Fall muss genau geprüft werden, ob das Scannen des Datenverkehrs zwischen den Clients und Servern, insbesondere über das Internet, und eine (nur auf das Anzeigen möglicher Treffer beschränkte) Endpoint Detection and Response zur Erfüllung des Sicherheitsbedarfs ausreicht. Die Untersuchung der Dateien und Daten auf dem

Client stellt dann den nächsten Schritt dar, wenn sich Anhaltspunkte für ein Schadprogramm ergeben haben.

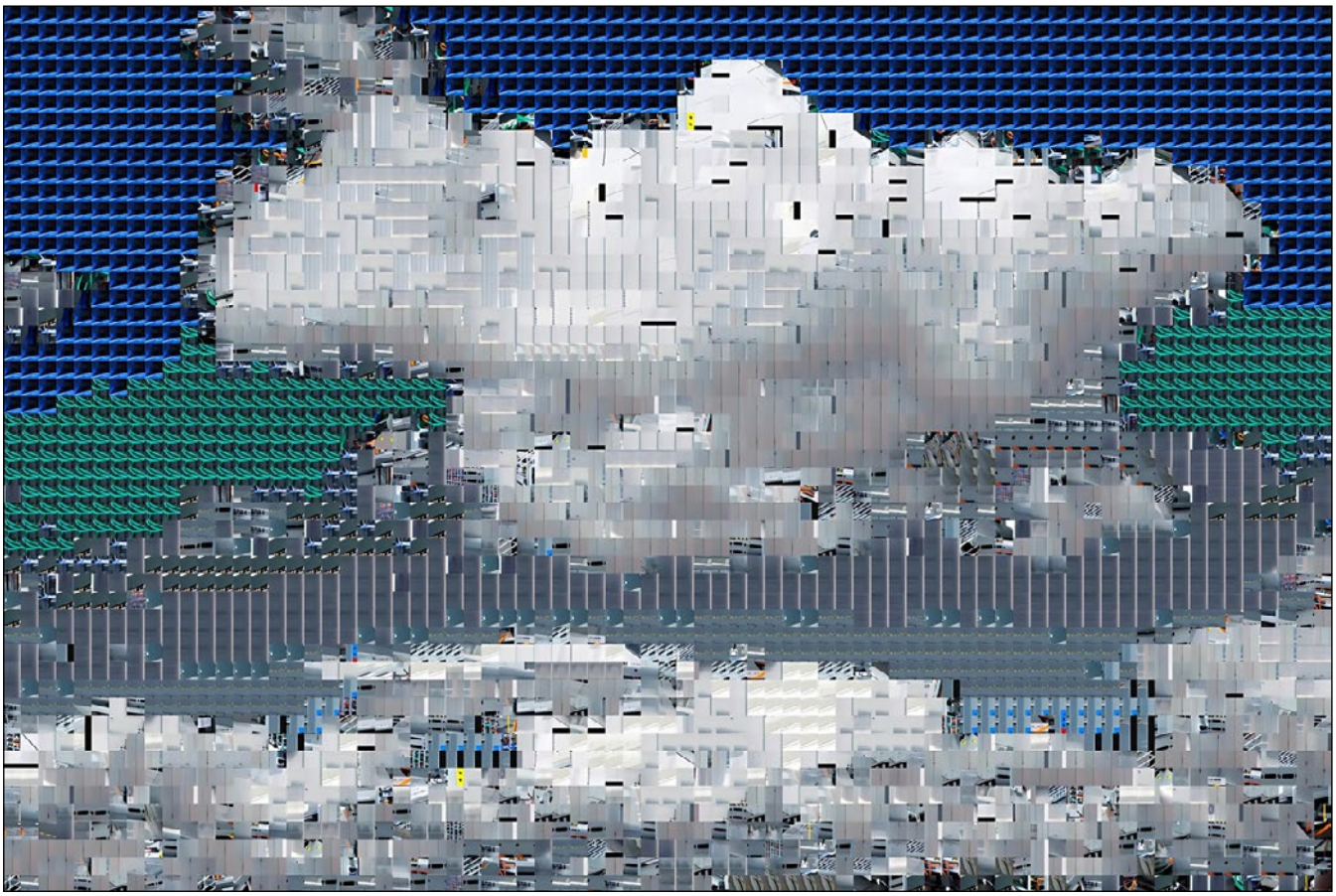
3. Die Durchführung einzelner Suchaufträge (Thread Hunting) in einem bestimmten Zeitraum ist grundsätzlich als ein milderes Mittel zu einer andauernden Überwachung (Monitoring / Hunt) bei gleicher Wirksamkeit vorzugswürdig.

4. Maßgeblich ist jedoch auch, wie Suchaufträge im Detail beschaffen sind (z. B. Suche nach dem Stichwort „Kündigung" in Dateien oder Ausgabe aller kürzlich erstellter Dateien eines Beschäftigten). Die Konfiguration trägt zur Zweckbegrenzung bei, wenn Suchaufträge sich nur auf IoC beschränken (z. B. anerkannte Malware-Signaturen) und nicht unnötig weitergehend sind. Eine lokale Prüfung (z. B. anhand spezifischer Suchaufträge) auf dem Client ist hierbei einer Übertragung ganzer Dateiinhalten an den Server vorzuziehen. Bearbeitende sollten im Ergebnis nur relevante Ergebnisse sehen.

5. Bei Anzeichen auf einen Befall eines bestimmten Geräts ist zu prüfen, ob anstelle einer interaktiven Durchsuchung über den Remote-Zugang, das Gerät nicht abgeschaltet und nach Benachrichtigung der betroffenen Beschäftigten lokal untersucht werden sollte. Dies trägt zur Transparenz beim Beschäftigten bei.

6. Besonderheiten können sich ergeben, wenn auch persönliche Daten von Beschäftigten (z. B. BYOD, eigene Dateien) oder Daten, die besonderer Geheimhaltung unterliegen, betroffen sind.

Nachdem wir die Verantwortlichen auf die Rechtslage hingewiesen hatten, konnten wir die Verfahren abschließen. Eine ergänzende Bewertung, Prüfung und Hinweise behalten wir uns aber vor.



Eine Cloud ist vor allem Technik und nicht eine schöne Wolke am Himmel. Wer auf Clouds setzt, sollte sich daher auch intensiv mit der Technik befassen.

☛ Weitere Informationen

BSI, IT-Grundschutzkompendium 2023:
bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

Recommandations de sécurité concernant l'analyse des flux HTTPS:
cyber.gouv.fr/publications/recommandations-de-securite-concernant-lanalyse-des-flux-https

7. Tätigkeitsbericht des Bayerischen Landesamt für Datenschutzaufsicht:
lda.bayern.de/media/baylda_report_07.pdf

Virenprüfung führt zu Veröffentlichung von Bewerbungsdaten

✎ Art. 57 Abs. 1 Buchst. f) DS-GVO

Bewerbungen hochladen und auf Viren prüfen? Wenn im Anschluss eines solchen Virenscans aber die Berwerbendendaten plötzlich online auffindbar sind, dann ist etwas schief gelaufen – und führt mitunter zu einer Verwarnung durch die Aufsichtsbehörde, wie der folgende Fall zeigt.

Durch eine anonyme Eingabe und eine Beschwerde sind wir darauf aufmerksam geworden, dass eine PDF-Datei einer Bewerbung über eine Suchmaschine im Internet auffindbar und abrufbar war. Die Bewerbung war auf zwei Webseiten veröffentlicht worden, bei denen man Dateien auf Viren überprüfen kann. Wir sind der Sache nachgegangen. Unsere Prüfung hat ergeben, dass ein Mitarbeiter der IT-Abteilung eines Unternehmens zur Prüfung von E-Mails mehrere Bewerbungen jeweils hochgeladen hatte. Dass die Inhalte in der kostenlosen Tarifstufe durch das Hochladen öffentlich zugänglich werden würden, war in den Produktbeschreibungen aufgeführt. Wir haben gegenüber dem Unternehmen deutlich gemacht, dass es sich um eine ernstere Angelegenheit handelt. Das Unternehmen hat die Datenpanne an uns im Anschluss gemeldet, die betroffenen Personen benachrichtigt, und war gehalten, sich um die Löschung (insbesondere auch nach Art. 17 Abs. 2 DS-GVO) auch bei den Drittanbietern (z. B. vorgenannte Webseiten, gängige Suchmaschinen, Webseiten-Cache-Dienste oder Internet-Archivdienste) zu kümmern. Wir haben eine Verwarnung ausgesprochen.

Aus unserer Sicht ist bei Verantwortlichen zwar häufig gewährleistet, dass bei Einkaufsprozessen kostenpflichtiger Dienste automatisch eine datenschutzrechtliche Überprüfung durch die zuständige Abteilung stattfindet, dies kann aber auch bei kostenlosen Diensten erforderlich sein. Gerade bei kostenlosen Webseiten, die keine Installation einer Anwendung unter erhöhten Rechten auf dem Endgerät voraussetzt, besteht das Risiko, dass Mitarbeitende auf Webseiten ungeprüfte Verträge für das Unternehmen schließen und personenbezogene Daten verarbeiten (z. B. LLM-Dienste, Übersetzungsdienste, Schreibverbesserungsdienste, File-Transfer-Cloud-Dienste, API-Entwicklerzugänge oder Social-Media-Dienste).

Verantwortliche sind gehalten, Mitarbeitende auf das Risiko einer nicht datenschutzkonformen Einbindung von Dritten hinzuweisen und Prozesse zu überarbeiten. Je nachdem, wie gravierend im Einzelfall sich ein Datenschutzverstoß darstellt, reagieren wir entsprechend unserer Abhilfebefugnisse nach Art. 58 Abs. 2. Idealerweise aber finden solche Datenschutzverstöße nicht statt durch datenschutzrechtlich angepasste Prozessabläufe der verantwortlichen Stelle. Wir selbst beraten lieber, als dass wir sanktionieren, und unterstützen Verantwortliche nach Möglichkeit. Wo aber notwendig, machen wir von unseren Abhilfebefugnissen Gebrauch.

Sensible Fragen auf Fragebogen zur Vorbereitung eines Bewerbungsgesprächs

✎ Art. 57 Abs. 1 Buchst. f) DS-GVO

Ein altes Problem in neuem Gewand: In einem Beschwerdeverfahren beschäftigte uns zum wiederholten Mal die Frage, welche Datenerhebungen vor bzw. in einem Bewerbungsgespräch zulässig sind. Dieses Mal aber mit einer Besonderheit.

Im Jahre 2024 erreichte uns eine Beschwerde, wonach ein Unternehmen in Baden-Württemberg zur Vorbereitung eines Bewerbungsgesprächs einen Fragebogen an die bewerbende Person ausgegeben hatte, auf dem unter anderem nach Krankheiten und Krankheitsfolgen, einer Schwerbehinderung, der Mitgliedschaft in einer Gewerkschaft, Pfändungen und Hobbys gefragt wurde. Außerdem wurden Name, Geburtsdatum und Beruf von Lebenspartner_innen und Namen und Geburtsdaten der Kinder erfragt. Auf dem Fragebogen fand sich ein Hinweis, dass das Ausfüllen freiwillig ist. Nach Anhörung des Unternehmens stellte sich heraus, dass es sich um einen Fragebogen aus der Zeit vor Inkrafttreten der DS-GVO im Jahr 2018 handelte. Nach Umstellung auf einen anderen Fragebogen waren nicht alle Exemplare entsorgt worden. Deshalb sei versehentlich in einer nicht mehr aufklärbaren Anzahl von Fällen der alte Fragebogen ausgegeben worden, ohne dass dies aufgefallen sei.

DS-GVO – auch ohne automatisierte Datenverarbeitung?

Die erste Frage, mit der wir uns im vorliegenden Verfahren beschäftigt haben, war die Anwendbarkeit der DS-GVO. Nachdem die durch die Fragebögen verarbeiteten personenbezogenen Daten soweit ersichtlich nicht mit Hilfe einer Datenverarbeitungsanlage verarbeitet wurden oder werden sollten, lag keine ganz oder teilweise automatisierte Verarbeitung nach Art. 2 Abs. 1 Var. 1 DS-GVO vor. Damit war für die Anwendbarkeit der DS-GVO gemäß Art. 2 Abs. 1 Var. 2 DS-GVO entscheidend, ob die Fragebögen, in denen die Daten nach den Kategorien „Persönliche Daten", „Kenntnisse & Fähigkeiten", „Gehalt / Kündigungsfrist" und „Sonstiges" geordnet waren, ein Dateisystem nach Art. 4 Nr. 6 DS-GVO darstellen. Dies haben wir bejaht.

Zulässige Fragen und No-Go-Bereiche

Damit war zu klären, ob für die Verarbeitung der personenbezogenen Beschäftigtendaten eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO bestand. Die Erhebung der von dem Fragebogen erfassten Daten konnte nicht auf eine Einwilligung der Bewerbenden nach Art. 6 Abs. 1 Buchst. a) DS-GVO gestützt werden. Nach Art. 4 Nr. 11 DS-GVO ist eine Einwilligung eine freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Bewerbende werden jedoch stets mit Nachteilen im Bewerbungsverfahren rechnen, wenn sie sich weigern, einen Bewerbungsfragebogen vollständig auszufüllen. Sie müssen befürchten, dass ein potentieller Arbeitgeber hieraus negative Rückschlüsse zieht. Dies gilt auch, wenn das Ausfüllen ausdrücklich als „freiwillig" bezeichnet wird. Damit ist nicht davon auszugehen, dass die Bewerbenden freiwillig und damit wirksam in das Ausfüllen des Fragebogens eingewilligt haben.

Die Erhebung von Gewerkschaftszugehörigkeit, Pfändungen, dem Vorliegen einer Schwerbehinderung, Lebenspartner_innen und Kindern sowie Hobbys war auch nicht nach Art. 6 Abs. 1 Buchst. b) Var. 2 DS-GVO zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen. Das Gleiche gilt für die pauschale Frage nach Krankheiten und Krankheitsfolgen. In einem Bewerbungsverfahren dürfen nur Fragen gestellt werden, welche für die Vertragsverhandlungen und damit die Entscheidung über die Einstellung der Bewerbenden notwendig sind. Ob eine Person Mitglied einer Gewerkschaft ist oder nicht, darf bereits aufgrund der Koalitionsfreiheit nach Art. 9 Abs. 3 Satz 2 GG die Einstellungsentscheidung nicht beeinflussen und ist daher im Bewerbungsverfahren irrelevant (BAG, Urteil vom 28. März 2000 – 1 ABR 16 / 99). Die Frage nach Pfändungen ist ebenfalls in der Regel unzulässig, sie käme nur in Betracht, wenn bei Kleinstbetrieben das Bearbeiten von Lohnpfändungen einen unzumutbaren Aufwand verursachen würde (s. ArbG Berlin, Urteil vom 16. Juli 1986 – 8 Ca 141 / 86). Das Vorliegen einer Schwerbehinderung darf im Bewerbungsverfahren ebenfalls nicht erfragt werden, maßgeblich ist alleine, ob die betroffene Person gesundheitlich in der Lage ist, die Anforderungen der Stelle zu erfüllen, so dass nur hiernach gefragt werden darf. Dies gilt bereits deshalb, weil eine Nichteinstellung wegen einer Schwerbehinderung, die die Eignung für die Stelle nicht betrifft, eine verbotene Diskriminierung nach § 7 Abs 1 Allgemeines

Gleichbehandlungsgesetz (AGG) wäre (LAG Hamburg, Urteil vom 30. November 2017 – 7 Sa 90 / 17). Auch nach Krankheiten und Krankheitsfolgen darf in Bewerbungsverfahren nicht pauschal gefragt werden. Zulässig ist nur die Frage, ob gesundheitliche Gründe der Ausübung der angestrebten Tätigkeit entgegenstehen und beispielsweise zu krankheitsbedingten Fehlzeiten führen werden. Angaben über Lebenspartner_innen, Kinder und Hobbies (soweit sie keinen Bezug zu dem angestrebten Beruf aufweisen) betreffen das Privatleben und haben keinen Einfluss auf die Eignung zur Ausübung einer beruflichen Tätigkeit. Nach diesen Informationen darf daher auch nicht im Bewerbungsverfahren gefragt werden. Es ist zu berücksichtigen, dass personenbezogene Daten im Bewerbungsverfahren nicht deshalb erfragt werden dürfen, weil sie nach Eingehung des Beschäftigungsverhältnisses relevant werden können.

Zudem dürfen personenbezogene Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht, und Gesundheitsdaten nur verarbeitet werden, wenn eine Ausnahme vom Verbot der Verarbeitung gemäß Art. 9 Abs. 1 DS-GVO vorliegt. Dass eine solche Ausnahme hier gegeben ist, war nicht ersichtlich. Insbesondere scheidet eine ausdrückliche Einwilligung der betroffenen Person nach Art. 9 Abs. 2 Buchst. a) DS-GVO aus den bereits im Zusammenhang mit Art. 6 Abs. 1 Buchst. a) DS-GVO genannten Gründen mangels Freiwilligkeit aus.

Zusammengefasst müssen Fragebögen zur Vorbereitung von Bewerbungsgesprächen so ausgestaltet werden, dass nur personenbezogene Daten erhoben werden, die für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich sind. Dies sind Informationen, die etwas über die Eignung des Bewerbenden für die ausgeschriebene Stelle aussagen. Daten, die vor dem Hintergrund des Antidiskriminierungsrechts bei Einstellungsentscheidungen nicht berücksichtigt werden dürfen, dürfen nicht erhoben werden.

„Ausmisten" als Datenschutzmaßnahme

Neben einem Verstoß gegen Art. 6 Abs. 1, Art. 9 Abs. 1 DS-GVO haben wir auch einen Verstoß gegen Art. 24 Abs. 1 und Art. 25 Abs. 1 DS-GVO festgestellt und deshalb eine Verwarnung ausgesprochen. Diese Normen verpflichten Verantwortliche dazu, die geeigneten und notwendigen technischen und organisatorischen Maßnahmen zu treffen, damit die Verarbeitung personenbezogener Daten im Einklang mit der DS-GVO stattfindet. Im vorliegenden Fall hätte das Unternehmen die veralteten Fragebögen aus dem Schrank der Auszubildenden entfernen müssen, um dafür zu sorgen, dass diese nicht ausgegeben werden und keine unzulässige Datenverarbeitung stattfindet. Von einer Geldbuße haben wir alleine deshalb abgesehen, da wir lediglich die Verwendung des Fragebogens in einem Fall nachweisen konnten und die unterlassene Entsorgung auf menschliches Versagen zurückzuführen war.

Zu einem funktionierenden Datenschutzmanagement-System gehört die fortlaufende Evaluierung von Risiken und die regelmäßige Sensibilisierung der Mitarbeitenden. Sehr wahrscheinlich wäre bei entsprechender Umsetzung aufgefallen, dass ein solch invasiver Fragebogen nicht zulässig sein kann.

© Illustration: Y. Dwiputri

Schulungszentrum und Veranstaltungen

BIDIB – Knapp fünf Jahre erfolgreiche Arbeit in unserem Bildungszentrum

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

Ein neues Jahr, eine neue Chance! In diesem Fall die Chance, das Bildungsangebot des Bildungszentrums weiter zu diversifizieren und sogar noch mehr Bürgerinnen und Bürgern sowie auch Vereinen, Behörden und Unternehmen die Möglichkeit zu geben, sich in Sachen Datenschutz und Informationsfreiheit weiterzubilden. Auch im Jahr 2024 gab es bei uns viele unterschiedliche Themen für viele unterschiedliche Zielgruppen.

Ein Jahr vor dem fünfjährigen Jubiläum des BIDIBs kann man zwei Dinge beobachten: Erstens, da wir nun bereits mehrere Jahre in Folge Veranstaltungen in Präsenz, online und auch hybrid anbieten, zeigt sich eine gewisse Routine. Wiederkehrende Prozesse wurden vereinfacht, die Medientechnik Stück für Stück ausgebaut und Standards in der Abwicklung festgelegt. Natürlich gilt es immer die Veranstaltungen zu organisieren, neue Themen zu finden und an der ein oder anderen Stellschraube zu drehen, jedoch es geht mitunter leichter von der Hand. Referent_innen werden angefragt, die Rahmenbedienungen geklärt, die Veranstaltung angekündigt und anschließend durchgeführt. Teilnahmebescheinigungen werden erstellt und die nächste Veranstaltung wird in Angriff genommen. Die Zahnräder machen, was sie sollen.

Zweitens, unsere Möglichkeiten wachsen! Seit nunmehr vier Jahren testen wir und schauen, auf welche Arten und Weisen unser Bildungszentrum funktionieren kann.

Begonnen mit den einfachen Onlineschulungen zu Zeiten der Coronapandemie über die hybriden Veranstaltungen in den neuen Seminarräumen der Behörde bis zu der Entwicklung neuer Bildungsformate sowie dem Bildungsportal, das nun endlich nächstes Jahr an den Start geht. Die Optionen für Bildung und unser Bildungszentrum sind groß. Wir arbeiten daran, die Struktur des Bildungszentrums grundlegend effizienter zu gestalten. Inspiriert durch das Projekt „Verwaltungstränsformer“ des Landes wurden sämtliche Prozesse analysiert und überarbeitet, um zukünftig mit derselben Anzahl an Stellen den Weg zu

noch mehr Veranstaltungen zu ebnen. Bisher konnte noch nicht alles technisch umgesetzt werden, und ein letzter Teil ist in Bearbeitung.

Da der Medienbereich verstärkt an den Videos des kommenden Bildungsportals arbeiten möchte, ist die Überarbeitung bestehender Prozesse weiterhin unerlässlich, um Seminare o. Ä. in ähnlicher oder höherer Frequenz gewährleisten zu können. Außerdem sollen zukünftig auch wieder kreative Projekte wie Trailer bzw. Clips begleitend zu bestimmten Schwerpunktthemen produziert werden – wie in der Vergangenheit zum Proctoring oder zur Informationsfreiheit.

Das BIDIB und der LfDI

Ohne die Behörde geht's nicht. Auch in diesem Jahr haben einzelne Personen, ganze Abteilungen sowie ich selbst als Dienstellenleiter das Bildungszentrum tatkräftig unterstützt. So wurde dieses Jahr beispielsweise „Keber Quarterly", ein Online-Videoformat, ins Leben gerufen. Nach positiven Rückmeldungen und erfreulichen Besuchszahlen wird dieses Format auch 2025 weiterbestehen.

Viele Abteilungen halten inzwischen regelmäßig Vorträge für das Bildungszentrum und locken immer weitere Interessierte in unser Haus. Doch auch außerhalb unserer Behörde sind unsere Fachleute aktiv. So gab es zum Beispiel Sonderschulungen für das Sozialministerium, nachdem Abteilung 3 unseres Hauses dort erheblichen Schulungsbedarf festgestellt hatte. Angeboten wurden Grundlagenschulungen und auch eine Vertiefungsschulung für den Sozialdatenschutz.

Damit wurde erreicht, dass neue Mitarbeitende des Sozialministeriums künftig direkt an datenschutzrechtlichen Schulungen unseres Hauses teilnehmen sollen und somit ein erster guter Schritt Richtung Grundsensibilisierung erreicht wurde.

Drei Jahre lang lief das Projekt „Schule digital", dessen Ziel es war, Datenschutz an Schulen zu stärken. Insbesondere allen am Schulleben Beteiligten wie Schulleitungen, Lehrkräften Sekretariaten, Eltern und Schüler_innen sollten Fortbildungen zugutekommen. Über 250 Veranstaltungen später mit ca. 4.370 Teilnehmer_innen kann man auf ein wirklich gelungenes und sinnvolles Projekt zurückblicken, das im Jahr 2024 mit 114 Veranstaltungen seinen Höhepunkt hatte. Wir werden dieses Themenfeld weiter zu bespielen, wenn auch in etwas kleinerem Umfang. Weitere 29 Veranstaltungen, die dieses Jahr liefen, besuchten insgesamt 2.600 Teilnehmende!

Insgesamt ungefähr 4.470 Personen besuchten dieses Jahr unsere knapp 150 Veranstaltungen. Ein kleiner Ausblick: 2025 feiert das Bildungszentrum für Datenschutz und Informationsfreiheit Baden-Württemberg sein fünfjähriges Jubiläum. Wir freuen uns darauf und damit auch auf die Veranstaltungen, die Projekte, die Kooperationen intern wie auch extern, die Erklärvideos – und auf neue Themen, die die Behörde, das Land und die Bürgerschaft beschäftigen.

www.baden-wuerttemberg.datenschutz.de/bidib-schule-digital

BvD-Herbstkonferenz und Behördentag 2024

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

Vom 16. bis zum 18. Oktober 2024 fand zum achten Mal die jährliche Datenschutzkonferenz des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. zum Thema „Regularien-Tsunami: Mit Sicherheit den Durchblick behalten" statt, die regelmäßig mit uns in Kooperation mit dem Landesamt für Datenschutzaufsicht (BayLDA) und dem Bayrischen Beauftragten für den Datenschutz (BayLfD) durchgeführt wird. In jährlichem Wechsel wurden in diesem Jahr wieder rund 250 Datenschutzbeauftragte aus dem öffentlichen (bDSBs) und privatwirtschaftlichen (DSBs) Bereich aus ganz Deutschland in Stuttgart begrüßt. Eine gute Gelegenheit, bei der unsere Mitarbeitenden zu verschiedenen aktuellen Fragestellungen mit den DSBs und bDSBs ins Gespräch kommen und wertvolle, konkrete Hinweise geben konnten.

LfDI Prof. Dr. Tobias Keber bei der BvD Herbstkonferenz in Stuttgart.

Im Gespräch: LfDI-Abteilungsleiterin Elisabeth Braun-Jäger und Prof. Dr. Tobias Keber.

Team LfDI in der Pause: LfDI Prof. Dr. Tobias Keber (Mitte, vorne) bespricht sich mit seinem Team, das zahlreiche Vorträge bei der Herbtskonferenz gehalten hat.

Abteilungsleiterin Elisabeth Braun-Jäger beim Vortrag zur aktuellen Rechtsprechung im Sicherheitsbereich.

Beliebtes Format bei der Konferenz: Das Publikum fragt, LfDI Prof. Dr. Tobias Keber antwortet.

Wie der Titel der Konferenz schon andeutete, wurden die zahlreichen EU-Rechtsakte (Data Act, Digital Services Act, NIS-2, Data Governance Act) und die damit verbundenen Herausforderungen für DSBs aufbereitet, ebenso wie die KI-Verordnung in verschiedenen Kontexten, z. B. im Beschäftigungsverhältnis oder aus Sicht des Staatsministeriums BW mit Blick auf Innovation, vertreten von Björn Beck (Leiter des Innovationslabors der Landesregierung). Genauso fanden wie üblich auch Vorträge zur Cybersicherheit großen Anklang. So konnte Nicole Matthöfer (Präsidentin der Cybersicherheitsagentur BW) einen besonderen Akzent zum Thema „Daten schützen – Cybersicherheit stärken" am Behördentag setzen. Jährlich wiederkehrend und damit Dauerbrenner der behördenspezifischen Themen waren auch wieder Social Media oder ein Überblick über die aktuelle Rechtsprechung.

Anlässlich der Konferenz veröffentlichten wir unsere im letzten Jahr angekündigte Aktualisierung der „Rechtsgrundlagen im Datenschutz beim Einsatz von KI, Version 2.0" sowie eine deutsche Version der europäischen Guidelines zu Deceptive Design Patterns als FAQs. Darüber hinaus konnten Problemstellungen aus der Praxis direkt an die Landesbeauftragten adressiert werden – in den beliebten Gesprächsrunden „Die Aufsichtsbehörde beantwortet Ihre Fragen", in denen ich gemeinsam mit dem Kollegen Michael Will des Bayerischen Landesamtes für Datenschutzaufsicht für jegliche Fragen von Unternehmensvertreter_innen zur Verfügung stehen, bzw. sich am Behördentag gemeinsam mit dem Kollegen Dr. Thomas

Petri den Anliegen öffentlicher Stellen annehmen. Zudem konnte ich als LfDI BW in Vorträgen Fragestellungen zu „Chancen und Herausforderungen von KI in der Verwaltung“ thematisieren und über Einsatz von Hochrisiko-KIs informieren.

Privacy by Design: Datenschutz in der europäischen Datenökonomie

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

Am 22. Oktober 2024 veranstaltete die TU München unter Federführung von Prof. Dr. Paal gemeinsam mit der Kanzlei Baumgartner Baumann Rechtsanwälte eine Diskussionsveranstaltung, zu die Hausleitungen aus Baden-Württemberg, Schleswig-Holstein und des Bayerischen Beauftragten für Datenschutzaufsicht eingeladen waren. Es war ein erfolgreiches Treffen mit der Kollegin Dr. h.c. Marit Hansen und dem Kollegen Michael Will sowie zahlreichen Verantwortlichen aus der Wirtschaft, Wissenschaft und Verwaltung.

Im Mittelpunkt der Veranstaltung stand Art. 25 DS-GVO. Nach Impulsen aus Sicht der Aufsichtsbehörden und Einblicken in die Aufsichtspraxis, wurden Fragen nach praktischer Relevanz von Art. 25 DS-GVO gestellt mit Blick auf konkrete Umsetzungs- und Dokumentationserwartungen an Unternehmen oder bzgl. Sanktionserfahrungen wegen Verstoß nach Art. 25 DS-GVO. Im Anschluss und als Mittelpunkt der Veranstaltung folgte ein neuartiges modifiziertes World Café-Format: Für die Diskussionsrunden, in denen jeweils ein oder eine LfDI mit einem Unternehmensvertreter aus Baden-Württemberg (SAP, Mercedes-Benz Group AG und Health Data Technologies GmbH) aktuelle Herausforderungen im Spannungsverhältnis der EU-Datenstrategie mit der DS-GVO diskutierten, wurde den Behördenleitungen jeweils ad hoc ein Unternehmensvertreter als Diskutant zugelost, was die Diskussion belebte und neue Perspektiven aufzeigte. Durch das direkte Gespräch der Behördenleitungen mit den Konzern-Datenschutzbeauftragten konnten konkrete Herausforderungen aus der Praxis ebenso wie aufsichtsrechtliche Anforderungen adressiert und für ein breites Fachpublikum zugänglich gemacht werden. So konnte das anwesende Fachpublikum aus Unternehmen und Kanzleien Best Practice-Beispiele von Unternehmen, die uns in Baden-Württemberg schon seit vielen Jahren in die Beratung von Technologieinnovationen einbeziehen, mitnehmen.

Thementag Internationaler Datentransfer

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

Die Schaffung eines neuen Transfermechanismus für die USA im Sommer 2023 (EU-US Data Privacy Framework) haben wir zum Anlass genommen, im Frühjahr 2024 bei einer öffentlichen ganztägigen Veranstaltung das Thema internationaler Datentransfer aus unterschiedlichen Blickwinkeln näher zu beleuchten.

Präsident BayLDA Michael Will, Prof. Dr. Boris Paal, LfD Schleswig-Holstein Dr. h.c. Marit Hansen, LfDI Prof. Dr. Tobias Keber, Dr. Johannes Baumann (v.l.n.r.).

v.l.n.r.: LfDI-Abteilungsleiter Alvar Freude, persönliche Referentin des LfDI Dr. Clarissa Henning, LfDI Prof. Dr. Tobias Keber, LfDI-Referent Dr. Jens Jacobi, Susanne Dehmel, Bitkom e.V.; Sebastian Greß, Konzerndatenschutzbeauftragter Mercedes-Benz Group AG.

Neben einer Einführung in das Thema und Vorträgen zum internationalen Datentransfer aus der Sicht eines weltweit tätigen Konzerns, der deutschen Digitalwirtschaft, der Rechtsberatung, der Europäischen Kommission und einer Verbraucherschutzorganisation stieß vor allem eine Diskussionsrunde zwischen einer Vertreterin der Europäischen Kommission und einem Vertreter der Organisation NOYB zur neuen Angemessenheitsentscheidung für die USA und ihren Folgen für Datenexporteure in Deutschland und Europa auf reges Interesse der zahlreichen Teilnehmenden vor Ort und online.

☛ Weitere Informationen

Leitlinien 05 / 2021 über das Zusammenspiel zwischen der Anwendung des Art. 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DS-GVO, Version 2.0, angenommen am 14. Februar 2023: edpb.europa.eu/system/files/2023-09/edpb_guidelines_05-2021_interplay_between_the_application_de.pdf

EDPB: Government access to data in third countries, Final Report, November 2021 – Indien, Russland, China: edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf

EDPB: Government access to data in third countries II, Final Report, April 2023 – Brasilien, Mexiko, Türkei: edpb.europa.eu/system/files/2023-10/study_on_government_access_to_data_in_third_countries_17042023_brazil_final_report_milieu_redacted.pdf

Empfehlungen 01 / 2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0 vom 18. Juni 2021: edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf

Opinion 22 / 2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), adopted on 7 October 2024: edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-222024-certain-obligations-following_en

Alle Bilder: © LfDI BW

Wie geht es weiter mit dem EU-US-Datentransfer? Das war eine der Fragen des Thementags. Das Bild ist mit Einwilligung der Abgebildeten entstanden ;).

Kommunaler Fachtag 2024

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

1.101 Gemeinden, davon neun Stadtkreise und 95 Große Kreisstädte, sowie 35 Landkreise – und das allein in Baden-Württemberg. In all diesen Stellen werden eine Vielzahl an öffentlichen Aufgaben bearbeitet. Teilweise handelt es sich um gesetzliche Pflichtaufgaben, teilweise übernehmen kommunale Stellen auch freiwillige Aufgaben, um ihre Bürger_innen zu unterstützen. Als Querschnittsmaterie tauchen Fragen zum Datenschutz und zur Informationsfreiheit dabei auf allen Ebenen auf. Vonseiten der Entlastungsallianz Baden-Württemberg wird wiederholt kolportiert, dass Datenschutz zur besonderen Herausforderung als Bürokratietreiber für öffentliche Stellen werde. Nicht selten wird deshalb gefordert, datenschutzrechtliche Auflagen zu minimieren. Aufseiten der Bürger_innen lassen sich die Erwartungen gegenüber Verantwortlichen bzgl. des Schutzes ihrer Daten gegenteilig feststellen. Laut einer aktuellen Studie „Künstliche Intelligenz und Kompetenz“, gefördert vom Bundesfamilienministerium, bei der 2.006 Personen ab 12 Jahren befragt wurden, messen 97 Prozent der Befragten dem Schutz der eigenen Online-Daten eine (große) Bedeutung zu, sind sich aber unsicher, inwieweit Verantwortliche für diesen Schutz sorgen. Für ein souveränes Leben in der digital vernetzten Welt wird der Datenschutz als hochrelevantes Thema eingeschätzt.

Um sich den divergierenden Ansprüchen zu widmen, veranstalteten wir am 5. November einen „Kommunalen Fachtag 2024“. In einer Diskussionsveranstaltung sollte über die beschriebene Kritik gesprochen werden, daneben sollten aber auch Positivbeispiele an öffentlichen Stellen ausgezeichnet werden, die Datenschutz (und Informationsfreiheit) konstruktiv umsetzen und Best Practices für andere Behörden liefern können.

Zur Podiumsdiskussion waren Dezernent Norbert Brugger, Vertretung der Kommunalen Landesverbände, und Dr. Falk Ebinger, Leiter der Geschäftsstelle der Entlastungsallianz, eingeladen, um gemeinsam mit mir die Forderungen an Datenschutz und Informationsfreiheit im Kontext von Bürokratieabbau zu erörtern. Innerhalb der Diskussion wurde deutlich, dass Bürokratie zunächst nicht grundsätzlich negativ zu bewerten sei, da diese für Rechtssicherheit und Regelbasiertheit sorge, wodurch staatliches Handeln vorhersehbar und nachvollziehbar ist. Ein Übermaß an Bürokratie (Bürokratisierung) erschwere jedoch die effiziente und veränderungsfreundliche Arbeit in öffentlichen Stellen. Die anwesenden Gäste – zum Großteil Mitarbeitende aus öffentlichen Stellen in Baden-Württemberg – machten deutlich, dass datenschutzrechtliche Fragestellungen und Anforderungen per se nicht für eine Überlast sorgen würden, sondern vielmehr, dass hierfür nicht genügend Ressourcen (Personal, Weiterbildung, Finanzmittel) zur Verfügung gestellt werden. Vielmehr würde Datenschutz als Zusatzaufgabe fachfremden bzw. nicht ausgebildeten Mitarbeitenden zugeteilt werden. Das sorge für Frustration bei

© LfDI BW

Zufriedener kommunaler Champion: Dieter Maier von der Stadt Stuttgart.

den Zuständigen. Die anwesenden behördlichen Datenschutzbeauftragten (bDSB) erschienen einhellig der Meinung, dass Datenschutz nicht zum Problem im Arbeitsalltag werde, wenn die Behördenleitung dahinterstehe. Dadurch könnten Arbeitsstrukturen geschaffen werden, in die Datenschutz bereits organisatorisch eingebettet sei, sodass die bDSB nur bei Spezialfragen hinzugezogen werden müssten. Auch das Podium war sich einig, dass Datenschutz demokratische Strukturen schützt und gemeinsam praktikable Lösungen gefunden werden müssen, die Innovation mit Datenschutz ermöglichen.

Im Anschluss an die Diskussion wurden zum zweiten Mal die Kommunalen Champions 2024 im Bereich Datenschutz, erstmalig auch im Bereich Informationsfreiheit, ausgezeichnet. Unser Wettbewerb hatte von April bis September öffentliche Stellen dazu aufgerufen, Ideen und Projekte einzureichen, wie Datenschutz und Informationsfreiheit leichter zugänglich, routiniert umsetzbar oder einfacher erklärt werden können – entweder innerhalb des eigenen Behördenalltags oder für Bürger_innen. Da die Einreichungen in diesem Jahr wieder so vielfältig und von hoher Qualität waren, entschied sich die Fachjury, bestehend aus Vertreterinnen und Vertretern der drei kommunalen Spitzenverbände Städte-, Landkreis- und Gemeindetag und dem Landesbeauftragten, dazu, neben jeweils einem Kommunalen Champion für Datenschutz und Informationsfreiheit zwei Sonderpreise zu verleihen. Im Bereich Datenschutz wurde das Landratsamt Neckar-Odenwald-Kreis (bereits zum zweiten Mal) zum Kommunalen Champion gekürt – dieses Mal für sein „Datenschutz-Wiki“. Über den Sonderpreis konnte sich die Stadt Stuttgart freuen, deren ganzheitlicher Ansatz einer Art Organisationsuntersuchung im Bereich Datenschutz Vorbildcharakter hat.

Weitere Informationen

Kompass: Künstliche Intelligenz und Kompetenz 2023. Einstellungen, Handeln und Kompetenzentwicklung im Kontext von KI:
jff.de/veroeffentlichungen/detail/kompass-kuenstliche-intelligenz-und-kompetenz-2023-einstellungen-handeln-und-kompetenzentwicklung-im-kontext-von-ki

Veranstaltungen zum Datenschutz als Kulturaufgabe

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

Wir arbeiten an Kulturtechniken des Digitalen, Fragen zur Informationsgesellschaft und an Herausforderungen, die die Digitalisierung und mit ihr die Künstliche Intelligenz mit sich bringt. Wir verfolgen die maßgeblichen Entwicklungen in diesem Bereich, soweit sie sich auf den Schutz personenbezogener Daten auswirken. Wir vernetzen uns mit anderen Aufsichtsbehörden, Wissenschafts- und Kulturinstitutionen auch zur Information und Sensibilisierung der Öffentlichkeit. Wir unterstützen inter- und transdisziplinär beim Aufbau von digitalem Know-How und überführen Fachdiskurse in eine Sprache und Form für Bürgerinnen und Bürger. Die Beteiligung der jüngeren und älteren Menschen an den so wichtigen Diskursen wollen wir aktiv stärken. Schließlich geht es um ihr Grundrecht auf informationelle Selbstbestimmung.

13. Forum Digitale Lebenswelt in Speyer

Wir waren Kooperationspartner beim renommierten 13. Forum Digitale Lebenswelt am 18./19. April 2024 in Speyer. In diesem Jahr widmete sich das Forum unter dem Oberthema „Wie wollen wir im digitalen Zeitalter leben?“ dem Schwerpunkt KI in der öffentlichen Verwaltung. Neben einer rechtlichen Standortbestimmung (KI-Verordnung, Data Act und weitere Digitalakte) stand der gemeinwohlorientierte und nachhaltige Einsatz von Künstlicher Intelligenz im Fokus, für den insbesondere die Kommunen und Länder Vorbild sein können. Juristische Überlegungen, insbesondere zur KI-Verordnung, spielten ebenso eine Rolle wie technische und gesellschaftliche Aspekte. Die Fachtagung wird von der Deutschen Universität für Verwaltungswissenschaften gemeinsam mit den Landesdatenschutzbeauftragten aus Rheinland-Pfalz und Baden-Württemberg sowie dem rheinland-pfälzischen Ministerium für Arbeit, Soziales, Digitalisierung und Transformation veranstaltet. Rund 200 Teilnehmerinnen und Teilnehmer haben die Veranstaltung vor Ort oder online besucht. Das Forum hat sich in den vergangenen Jahren mit der Qualität seiner Vorträge, aber auch als Ort des Austausches und der Diskussion einen Na-

men in der Fachwelt gemacht. Nach zwei Jahren Pause beteiligen wir uns seit dem Jahr 2024 wieder an der Programmplanung.

> ☛ **Weitere Informationen**
>
> www.baden-wuerttemberg.datenschutz.de/speyerer-forum-zur-digitalen-lebenswelt-am-18-und-19-april

Kultur vernetzt – Der LfDI in der Stadtbibliothek

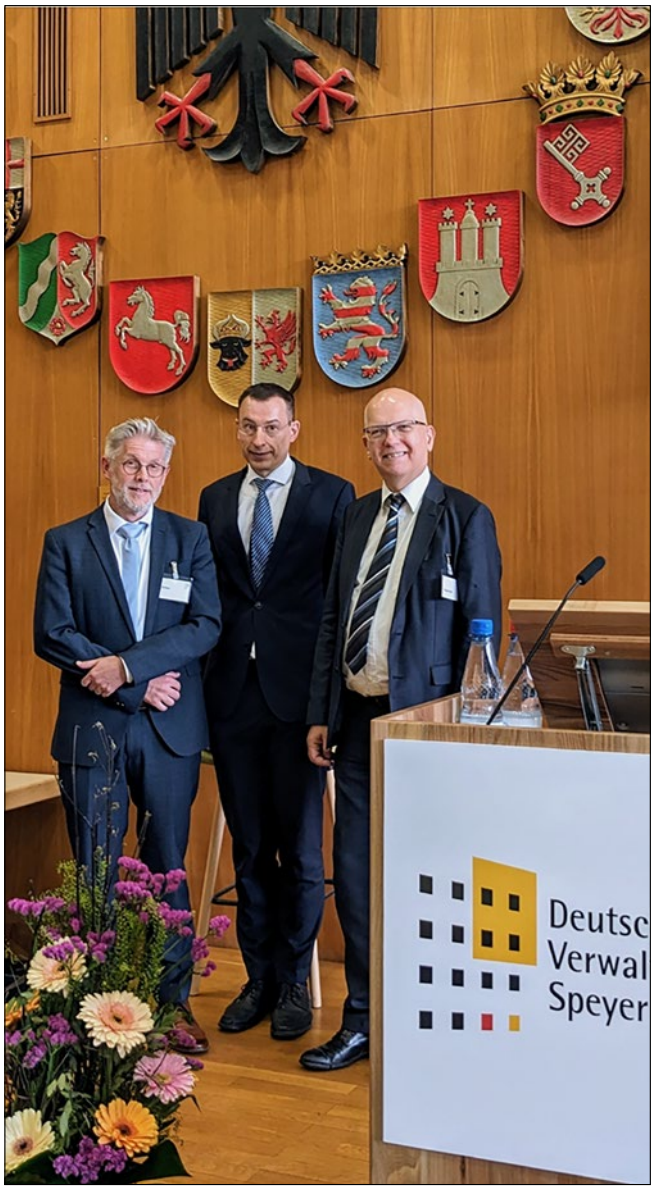
Weiter arbeiten wir an Kooperationen mit anderen Einrichtungen zu Digitalisierungsthemen. So waren wir Partner einer Veranstaltung in der Stadtbibliothek, zusammen mit der Landeszentrale für Politische Bildung.

Eva Wolfangel hielt einen Vortrag „KI und Fake News“ und sprach im Anschluss mit der Moderatorin Leonie Maderstein darüber, wie Fake News erkannt werden können, wie wir Fakten checken können und über den Unterschied zwischen von Menschen willentlich oder unwillentlich gemachten Fehlinformationen und solchen, die von KI-Anwendungen produziert werden.

> ☛ **Weitere Informationen**
>
> www.baden-wuerttemberg.datenschutz.de/ki-und-fake-news-vortrag-und-gespraech-zum-nachhoeren

KI-Woche: KI und Datenschutz – Wer trainiert die Zukunft?

Wieder wurde aus der Mitte der Dienststelle die KI-Woche organisiert und ein vielfältiges und fachlich fundiertes Programm zusammengestellt. Vom 30. September bis zum 2. Oktober hielten Expert_innen Vorträge, diskutierten auf Panels und mit dem Publikum. Die Teilnahme war wie gewohnt vor Ort und online möglich, die KI-Woche begrüßte dabei vor Ort bis zu 60 Personen, online bis zu 130 Personen.



© LfDI RLP

V.l.n.r.: LfDI Prof. Dr. Tobias Keber, Prof. Dr. Mario Martini, LfDI Prof. Dr. Dieter Kugelmann.

© LfDI BW

Eva Wolfangel sprach in der Stadtbibliothek über Fake News.

Als lernende Behörde möchten wir mit diesem Format einerseits Fachexpertise zu uns ins Haus holen. Gemäß Art. 57 Abs. 1 Buchst. i) DS-GVO sind wir gehalten, die maßgeblichen Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken. Andererseits geben wir unser Wissen an ein Fachpublikum weiter und adressieren zugleich die breite Öffentlichkeit, um gemäß Art. 57 Abs. 1 Buchst. b) DS-GVO für unsere Themen zu sensibilisieren und aufzuklären.

Infokasten

Das Programm und die Videos der KI-Woche 2024 stehen hier: www.baden-wuerttemberg.datenschutz.de/ki-woche-2024

Illustration: Y. Dwiputri

Tag eins: Eröffnungskeynote, KI-generierte Audiokunst und Science-Slam

Den Vorspann zur Themenwoche bildeten auch dieses Jahr interdisziplinäre gesellschaftliche Fragestellungen zu KI und dem sozio-technischen Gefüge.

Eva Wolfangel fragte in der Erföffnungskeynote „Human as a Service – Die andere Seite der Zukunft" nach der menschlichen Arbeit, die in künstlichen intelligenten Systemen steckt und die immer neu aufgewendet werden muss, um sie an sich ändernde Datenlagen und Zielsetzungen anzupassen. Kontrolliert hier der Human in the Loop die Maschine – oder ist er viel eher der wenig autonome Serviceleistende in einem Funktionskreislauf?

Ebenfalls Tradition hat zum Auftakt unserer Veranstaltung der Blick auf künstlich-intelligente Technik durch die Arbeit von Künstler_innen. Professor Ephraim Wegner stellte das von ihm mit Dr. Daniel Bisig entwickelte Tool Deep Dream Audio vor, das akustische Ereignisse kopiert, anreichert und in neuen Formen ausspielt. Künstlerisch angewendet hat Wegner diese Software mit dem Komponisten und Musiker Thomas Wenk.

Zum Abschluss des ersten Tages präsentierten Nachwuchswissenschaftler in einem Science-Slam inszenierte Einblicke in Aspekte von digitaler Regulierung sowie in Fragen von Nachhaltigkeit und KI.

Fachtag KI: Beschäftigtendatenschutz – Gesundheitsdaten – Bildung / Social Media, Use Cases und Film

Der zweite Tag der KI-Woche stand im Zeichen von Vorträgen zu den Themenblöcken Beschäftigtendatenschutz, Gesundheitsdatennutzung und im weitesten Sinne dem der Bildung: dem oft ungeschützten Social-Media-Alltag von Kindern und Jugendlichen.

KI in der Rechtspraxis: Work in Progress

Den Auftakt machte RAin Nina Diercks, die zunächst provokativ in Frage stellte, ob der Anwendungsbereich der KI-Verordnung denn überhaupt so umfassend gegeben sei, wie er diskutiert wird, um dann den HR-Bereich als Hochrisiko-Bereich unter die Lupe zu nehmen. Wann genau ist hier der Anwendungsbereich der KI-VO eröffnet? Welche Pflichten ergeben sich hieraus für Anwender_innen? Welche Rückausnahmen gelten? An Diercks Vortrag schloss sich eine kontroverse Diskussion um die Definition von KI im AI Act (Art. 3) und um weitere Präzisierungen in den Erwägungsgründen (ErwG 12) an.

Zweckbindung in der Gesundheitsdatenforschung und Teilhabeorientierung

Im Vortrag „Gesundheitsdatennutzung im Spannungsfeld von Forschung, Innovation, klinischer Versorgung und Ethik" von Prof. Dr. Philipp Kellmeyer ging es um Innovationen, die mobile medizinische Anwendungen oder die großflächige Erhebung von Patient_innendaten versprechen, um Zugang zu und Schutz von Daten, um mögliche Formen von Einwilligung und Zweckbindung und um den Ansatz partizipations- und teilhabeorientierter Forschung, etwa: Wer sollte mitbestimmen, wenn z. B. Leitlinien zur Etablierung einer verantwortungsvollen Künstlichen Intelligenz erstellt werden? Im sich anschließenden Gespräch mit Dr. Jan Wacke ergänzten beide die datenschutzrechtliche Diskussion der vergangenen Jahre auch um ethische und sozialpolitische Aspekte in der Gesundheitsdatenforschung.

KI, Psyche und Jugendschutz

Dr. Dorothe Dörholt, Filmemacherin und Psychologin, griff in ihrem Vortrag psychologische Wirkmechanismen (Lernmechanismen) auf, die gezielt in Internetapplikationen einprogrammiert sind und die informationelle Selbstbestimmung unterlaufen. Von hier ausgehend berichtete sie aus ihrer aktuellen psychologischen Praxis von der Suchtgefahr, der Kinder und Jugendliche bei Social Media-Anbietern gezielt ausgesetzt sind, und appellierte an das Verantwortungsbewusstsein von Eltern diesbezüglich.

LfDI a.D. Dr. Stefan Brink fragte in seinem Vortrag nach dem sich im steten Wandel befindlichen Konzept von Kindheit als historisches und soziales Konstrukt. Aus diesem müsse eine Gesellschaft Schutzrechte von Kindern ableiten und durchsetzen. Wie sind hier die rechtlichen Möglichkeiten des Ju-

© LfDI BW

LfDI Prof. Dr. Tobias Keber (links) im Gespräch mit Regisseur Martin Mannweiler.

gend(Daten)Schutzes überhaupt einzuschätzen? Was steht dazu in der DS-GVO und was in der KI-Verordnung?

Use Cases: Hands-on aus dem Ländle

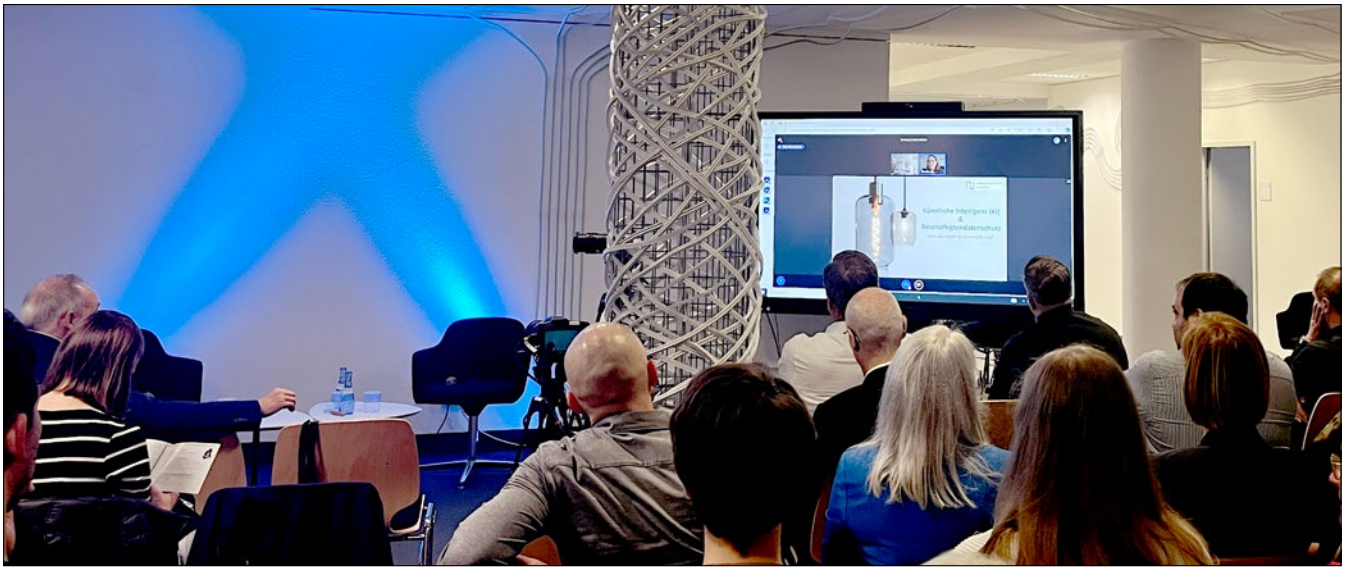
Die folgenden „Hands-on-Präsentationen" lieferten Einblicke, wie mit den (datenschutzrechtlichen) Herausforderungen von KI in der Praxis umgegangen wird. RA Marius Drabiniok gab einen Werkstattbericht aus der Rechtspraxis zu den europäischen Rahmenbedingungen von KI, Zina Al-Washash und Professor Dr. Thomas Schuster von der Uni Pforzheim stellten ihr Forschungsprojekt „Künstlich-intelligente Verbraucherdurchsetzung" vor und Steffen Haschler, Gymnasiallehrer und Hacker, zeigte einen KI-gestützten Selbstlernkurs für den Informatikunterricht.

Kinoabend: Pilotprojekt der Videoüberwachung in Mannheim

Zum Abschluss ging´s ins StadtPalais. Dort schauten wir gemeinsam den Filmessay „Algorithmenbasierte Kameraüberwachung" (D 2022) von Regisseur Martin Mannweiler, der ein polizeiliches Pilotprojekt in Mannheim zur algorithmenbasierten Überwachung öffentlicher Räume dokumentiert. Im Anschluss sprachen wir mit dem Regisseur und luden das Publikum zur Diskussion ein. Der Filmabend war eine Kooperation mit dem StadtPalais – Museum für Stuttgart und der Stadtbibliothek Stuttgart.

Der dritte Tag: AI-Literacy – Workshops und Panel

Wie in Art. 1 Abs. 1 der KI-Verordnung dargestellt sollen KI-Systeme im Einklang mit den Werten der Europäische Union stehen. Hierzu soll menschenzentrierte und vertrauenswürdige Künstliche Intelligenz gefördert und ein hohes Schutzniveau ange-



© LfDI BW

Kein Problem für die Technik: Nina Diercks konnte kurzfristig nicht nach Stuttgart kommen. Also wurde sie live zugeschaltet. Die Debatte darüber, wann die KI-Verordnung im Beschäftigtenkontext greift, wurde auch über die Distanz intensiv geführt.

sichts möglicher Risiken durch KI erreicht werden. Der Artikel nennt Gesundheit und Sicherheit als zentrale zu schützende Bereiche, ergänzt um den Schutz der in der Charta der EU verankerten Grundrechte, ebenso den Schutz vor schädlichen Auswirkungen. Hier zeigen sich deutlich die Schnittstellen zum Datenschutz, die ebenfalls Ausdruck in Art. 4 KI-VO durch die Maßgabe einer KI-Kompetenz (AI-Literacy) bekommen.

So stand der dritte Tag der KI-Woche ganz unter dem Motto der AI-Literacy, die datenschutzrechtliche mit technischen, sozialwissenschaftlichen und ethischen Kenntnissen verknüpft.

Was will die KI-Verordnung?

Art. 1 Abs. 1

Zweck dieser Verordnung ist es, das Funktionieren des Binnenmarkts zu verbessern, indem ein einheitlicher Rechtsrahmen insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union im Einklang mit den Werten der Union festgelegt wird, um die Einführung von menschenzentrierter und vertrauenswürdiger künstlicher Intelligenz (KI) zu fördern und gleichzeitig ein hohes Schutzniveau in Bezug auf Gesundheit, Sicherheit und der in der Charta der Grundrechte der Europäischen Union („Charta") verankerten Grundrechte, einschließlich Demokratie, Rechtsstaatlichkeit und Umweltschutz, sicherzustellen, den Schutz vor schädlichen Auswirkungen von KI-Systemen in der Union zu gewährleisten und gleichzeitig die Innovation zu unterstützen.

eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32024R1689

Wie im vergangenen Jahr konnten vor Ort Workshops belegt werden, angeboten von Referent_innen aus dem Haus und unter großem Zuspruch der Teilnehmer_innen. Dr. Peter Nägele thematisierte KI und Bias / Diskriminierung, Dr. Clarissa Henning lud zu einem Worldcafé zum Einfluss von KI auf Mediensysteme vor allem aus ethischer Perspektive, Dr. Walter Kicherer fragte, wie der KI-Einsatz in der Bildung rechtlich möglich sei, und Alvar Freude bediente live Bildgeneratoren.

Der Nachmittag schloss mit einem Abschlusspanel zu AI-Literacy. Hier zeigte man sich einig, dass Interdisziplinarität der Schlüssel sei, um wertebasierte KI-Innovation zu sichern.

Recht als geronnene Ethik

Vanessa Hanschke, Doktorandin an der Universität Bristol, stellte das Risikomanagement-Projekt „Data Ethics Emergency Drill" vor, das Verfahren des Designs, der Mensch-Maschine-Interaktion und der Cybersecurity integriert und mit dem „der Ernstfall" geprobt werden kann, z. B.: Was ist zu tun, wenn eine KI nach Aufspielen eines Updates ethisch unerwünschte Resultate produziert? Ziel ist es, abstrakte ethische Regeln (die hinter Grundrechten wie der informationellen Selbstbestimmung stehen) auf eine konkrete Praxis anzuwenden.

Professorin Dr. Petra Grimm zeigte, warum ethische Grundsätze beim Einsatz und bei der Entwicklung von KI-Anwendungen notwendig sind. Dabei übersetzte sie Begriffe, die die Moralphilosophie bis heute prägen, für den Umgang mit Künstlicher Intelligenz: *Klugheit („Klug ist, wer die Perspektive der Betroffenen reflektiert, KI maßvoll einsetzt und sich nicht dem Diktat des Effizienzdenkens unterwirft"), Maßhalten („Datenminimierung"), Mut („nicht alles technisch Mögliche ist sinnvoll"), Gerechtigkeit (Biases minimieren, Auswirkungen auf Mensch und Natur und den sozialen Zusammenhalt im Blick behalten).*

Im abschließenden Podium reflektierten wir zusammen mit beiden Vortragenden und mit dem Publikum unter der Moderation meiner persönlichen Referentin Dr. Clarissa Henning, inwiefern

Data-Mining beudetet etwas völlig anderes, als in einer Mine nach Rohstoffen zu suchen.

rechtliche Normen – sei es mit der KI-Verordnung oder der DS-GVO – europäischen Wertemaßstäben Ausdruck verleihen und dafür sorgen, dass diese auch für KI-Innovation gelten.

Unsere KI-Woche wird in Baden-Württemberg gesehen und geschätzt. Wir vernetzen zentrale Akteure in Baden-Württemberg und sehen und hören als beratende Aufsichtsbehörde aus erster Hand, wie der Stand der KI-Entwicklung in den jeweiligen Sektoren ist und wo der Schuh drückt. So nützt die KI-Woche nicht nur den Fachleuten der Behörden und Unternehmen sowie der Bürgerschaft, sondern auch uns selbst.

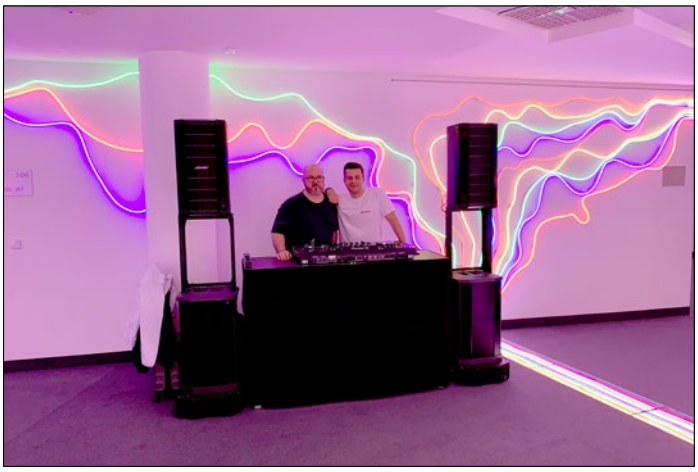
Die Lange Nacht der Museen

Eine unserer Kernaufgaben besteht darin, Bürger_innen bei der Durchsetzung ihrer Betroffenenrechte im Datenschutz zu unterstützen. Wir stellen jedoch häufig fest, dass viele Menschen diese Betroffenenrechte gar nicht kennen und auch den Landesdatenschutzbeauftragten und seine Arbeit nicht. Um einen niederschwelligen Zugang zum Thema und zur Behörde zu schaffen, haben wir nun im dritten Jahr mit der begehbaren Lichtinstallation „Data to Light" des Künstlers Florian Mehnert an der Langen Nacht der Museen 2024 teilgenommen. Auch in diesem Jahr konnten wieder über 1.000 Interessierte den Datenschutz (und auch die Informationsfreiheit) auf ganz neue Weise kennenlernen. Ein facettenreiches Programm konnte ganz unterschiedliche Zielgruppen ansprechen. Die Lichtkunst, begleitet von den elektronischen Beats der Stuttgarter DJs STR.711. KOLLEKTIV, begeisterte im Besonderen eine junge Zielgruppe, die am Pressestand ins Gespräch zum Datenschutz und zur Informationsfreiheit kam. Die Vorträge des Künstlers zu seinem Werk mit dem Hintergrund, Daten und die Arbeit mit Daten sichtbar zu machen, erfreuten sich bis in die späten

Nachtstunden großer Beliebtheit, ebenso wie die Sondervorträge des ehemaligen Landesbeauftragten Dr. Stefan Brink zu „Datenschutz in der Bildenden Kunst“. In jedem Jahr bringen sich auch die Mitarbeitenden aus unseren Fachabteilungen mit neuen Ideen ein, um Datenschutz und Informationsfreiheit zu präsentieren. In diesem Jahr wurden in Bilderrahmen an den Wänden der langen Flure die Vielseitigkeit der Datenschutz-Themen kurz und knackig dargestellt und mittels eines QR-Codes auf weiterführende Informationen verwiesen. Hierbei konnten teilweise mehrere hundert Zugriffe an dem Abend auf einzelne Themen verzeichnet werden. Das Rezept scheint aufzugehen, die Relevanz von Datenschutz für jede_n Einzelne_n greifbar zu machen und mit der Lebenswelt der Besucher_innen zu verknüpfen. Bei der Langen Nacht präsentierte Ephraim Wegner auch das Spiel „Colliding Objects“, eine Installation zum Mitspielen, die uns anregte, uns näher mit dem Projekt zu befassen.

© LfDI BW

Immer beliebt: Gespräche über die Einschränkung der Freiheitsrechte von Sport-Profis.



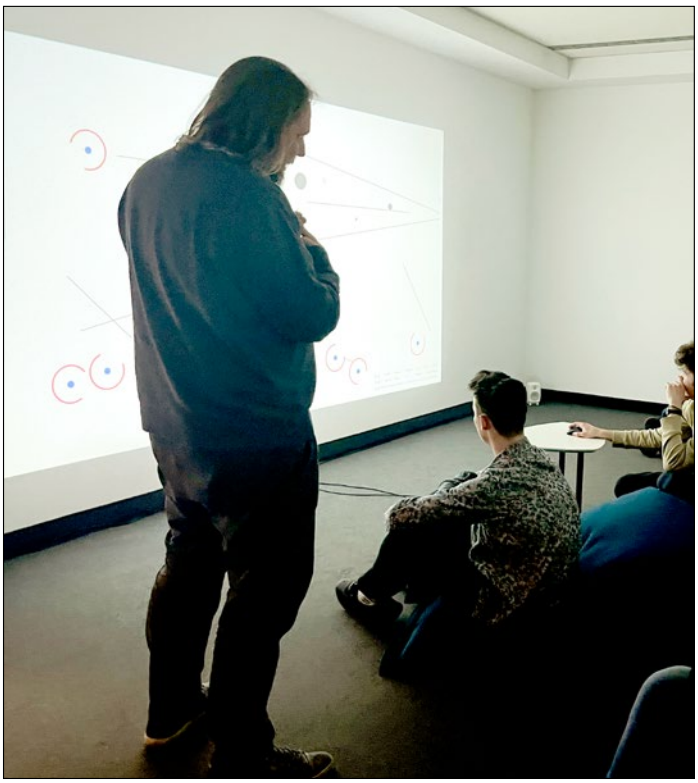
© LfDI BW

Nach dem Aufbau und vor dem Publikumsandrang: Die DJs an ihrem Arbeitsgerät.

Colliding Objects – Audiovisuelles Spiel und Visualisierung des Datenhandels

Mit der Macromedia Hochschule gingen wir im Sommersemester 2024 eine Kooperation ein. Bereits bei der Langen Nacht der Museen hatte uns Professor Ephraim Wegner ein mit Studierenden entwickeltes audiovisuelles Spiel vorgestellt, das vom Publikum interaktiv gespielt werden konnte. Physikalisch simulierte Objekte werden als „Colliding Objects“ genutzt, um sequenzielle Muster und Klangfolgen zu generieren.

In der Kooperation mit der Hochschule sollte dieses Spiel weiterentwickelt werden mit der Zielrichtung, das Spielverhalten durch ein entsprechend programmiertes Backend beispielhaft zu klassifizieren



© LfDI BW

Spielen und über Datenschutz und Technik sprechen – möglich bei der Langen Nacht.

Zu Gast bei LfDI Prof. Dr. Tobias Keber (3.v.l.): Prof. Ephraim Wegner (4.v.l.) und Studierende der Hochschule Macromedia aus dem Studiengang "Digital Technologies und Coding" stellten am 4. Juli die überarbeitete Version von "Colliding Objects" vor. Mit dabei die LfDI-Referentinnen Simone Markovic und Thuy Nga Trinh.

und auszuwerten und diesen Vorgang für die Spielenden erfahrbar zu machen. Am 4. Juli besuchte uns eine 7-köpfige Delegation des Seminars mit ihrem Seminarleiter und präsentierte ihre Arbeit. In unserer KI-Woche wiederum konnte Colliding Object 2.0 vom Publikum ausprobiert und die Kategorisierungen am eigenen Leib erfahren werden.

☛ Weitere Informationen

Shoshana Zuboff, Das Zeitalter des Überwachungskapitalismus, Frankfurt am Main / New York 2018.

Messen und Konferenzen

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

Auf der re:publika und der Secure Linux Administration Conference 2024 in Berlin und auf dem 38. Chaos Communication Congress (38C3) in Hamburg etwa waren unsere Expert_innen der Abteilung Technisch-organisatorischer Datenschutz und haben Vorträge gehalten. Auf diesen Veranstaltungen konnten wir unsere Themen diskutieren, etwa wie man mit Datenlecks umgeht, oder etwas unterhaltsamer mit unserer „Die große Datenschutz-, Datenpannen- und DS-GVO-Show“.

Wir lernen auch auf diesen Veranstaltungen dazu, nehmen Impulse auf. Immer wieder wird uns als staatliche Stelle auch klar, wie wichtig und hilfreich der Beitrag der Communities ist, und so manches Mal wundern wir uns, dass etwa freundliche Hinweise von Menschen auf Systemschwachstellen bei Behörden oder Unternehmen nicht dankend angenommen und umgehend die Lücken geschlossen werden, sondern sich gerade diese Menschen Kritik ausgesetzt sehen. Der sogenannte Hackerparagraf sollte eigentlich von der Bundesregierung noch in dieser Legislatur angepasst werden und Menschen schützen, die beim Aufspüren und Schließen von IT-Sicherheitslücken helfen. Dieses Vorhaben wurde nicht umgesetzt, was bedauerlich ist.

Auch nahmen unsere Fachleute an verschiedenen Veranstaltungen der Start-up-Szene teil wie dem Start-up BW Summit 2024, um mit jungen Unternehmener_innen ins Gespräch zu kommen. Wir wollen wirksam beraten, dafür ist der direkte Austausch sehr wichtig für uns (s. S. 85).

Weitere Informationen

rsw.beck.de/aktuell/daily/meldung/detail/computerstrafrecht-202a-stgb-hackerparagraf-it-sicherheitsforscher-strafbarkeit

38C3, Was tun, wenn man ein Datenleck entdeckt hat?
media.ccc.de/v/38c3-was-tun-wenn-man-ein-datenleck-entdeckt-hat

38C3, Die große Datenschutz-, Datenpannen- und DS-GVO-Show:
media.ccc.de/v/38c3-die-groe-datenschutz-datenpannen-und-ds-gvo-show

re:publika24, „Chatkontrolle" – Same same, but different, but still same?
re-publica.com/de/session/chatkontrolle-same-same-different-still-same

Secure Linux Administration Conference 2024":
heinlein-support.de/slac/2024/vortrag/das-grosse-datenschutz-und-datenpannen-quiz

Start-up BW Summit 2024:
summit2024.startupbw.de

Praxisorientierter Austausch bei der didacta in Köln

Wie wichtig der Austausch mit Fachleuten und Bürgerschaft ist, zeigt sich wie folgt auch am Beispiel unserer Teilnahme an der didacata.

Die Bildungsmesse didacta in Köln gilt als Treffpunkt für Pädagog_innen, Lehrkräfte, Erzieher_innen, und zahlreiche andere Bildungsexperten. Wir haben zusammen mit drei weiteren Aufsichtsbehörden (Hessen, Thüringen, Berlin) an der diesjährigen Messe als Aussteller mit einem gemeinsamem Stand teilgenommen. Die Bildungsmesse bot ein breites Spektrum an innovativen Ideen und Lösungsvorschlägen für die Herausforderungen im Bildungsbereich. Wir wollten mit unserer Präsenz vor Ort den Austausch fördern und mit der Fachszene ins Gespräch kommen. Unsere Fachleute von der Abteilung Bildungswesen waren präsent – und gefragt.

Den Stand besuchten Erzieher_innen, Lehrkräfte an Grund- und weiterführenden Schulen, Sozial- und Medienpädagog_innen sowie Schulsozialarbeiter_innen. Auch Hersteller von Schul-IT kamen für Beratungen an den Stand. Erfreulicherweise

© LfDI BW

Gemeinsam auf der Bildungsmesse didacta: Der LfDI BW informierte zusammen mit Fachleuten aus Berlin, Thüringen und Hessen über Datenschutz und Bildung.

© Frank Eppler

Datenschutz und KI: LfDI-Referent Daniel Maslewski, LL.M., sprach darüber bei KI.CKSTART.

ist das Thema „Datenschutz“ auch in der Start-up-Szene angekommen. Wir konnten auf individuelle Fragen eingehen und datenschutzrechtliche Tipps und Hinweise geben. Schließlich macht es der zunehmende Einsatz digitaler Medien im Bildungsbereich unabdingbar, dass Lehrkräfte über die neuesten Entwicklungen im Datenschutz informiert sind. Die Beratungen am Stand gaben Lehrkräften praktische Hinweise an die Hand, um einen sicheren und datenschutzkonformen Unterricht zu gestalten. Die Fortbildungen „Schule digital“ unseres Bildungszentrums für Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB) fanden ein großes Interesse. Direkt am Stand konnten wir in unzähligen Kurzberatungen und Gesprächen auf die Bedeutung des Datenschutzes aufmerksam machen und auf unser Fortbildungsangebot hinweisen.

Viele Fragen fokussierten sich auch auf die Förderung der Medienkompetenz in der Schule. Auf großes Interesse stießen deshalb die Broschüre „Datenschutz geht zur Schule“ mit Unterrichtsvorbereitungen für Lehrkräfte sowie das Videoformat „Datenschutz leicht erklärt“ vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., das in Kooperation mit uns aufgelegt wurde (wir berichteten in unserem 39. Tätigkeitsbericht Datenschutz 2023 darüber). In den kurzen Erklärvideos werden hier die komplexen Aspekte des Datenschutzes in der digitalen Welt für junge Menschen in Szene gesetzt. Wir unterstützen beide Projekte des BvD, gehen an Schulen, um über Datenschutz zu sprechen.

Auch das Angebot von YoungData stieß auf großes Interesse. YoungData ist ein Jugendangebot der Aufsichtsbehörden der Länder und des Bundes, das Themen des Datenschutzes und der Informationsfreiheit jugendgerecht aufbereitet online zur Verfügung stellt. Wir unterstützen die Arbeit von YoungData und beteiligen uns an der Redaktion. Für uns ist es wichtig, dass wir jungen Menschen in einer angemessenen Sprache informieren, aufklären und sensibilisieren.

Das Konzept „Data-Kids“ der Berliner Aufsichtsbehörde, das darauf abzielte, Kinder spielerisch und altersgerecht an das Thema Datenschutz heranzuführen, war bei Mitarbeitenden von Kindergärten und Grundschulen sehr begehrt. Die interaktiven Module erklärten den Kindern auf anschauliche Weise, wie sie ihre persönlichen Daten schützen können und sensibilisierten sie für einen verantwortungsbewussten Umgang mit digitalen Medien.

Insgesamt waren die Beratungen und Gespräche am Stand der Aufsichtsbehörden auf der didacta in Köln sehr facettenreich. Die praxisorientierten Angebote machten den Stand attraktiv für alle, die im Bildungsbereich tätig sind. Der Messestand der vier beteiligten Aufsichtsbehörden erhielt die erwünschte Resonanz. Deswegen planen wir, uns an der didacta 2025 wieder mit mehreren Aufsichtsbehörden zu beteiligen, und zwar diesmal in Stuttgart vom 11. bis zum 15. Februar.

KI.CKSTART mit Datenschutz – LfDI auf GenAI Event

Am 19. und 20. November 2024 hat der Bildungswerk der Baden-Württembergischen Wirtschaft e. V. gemeinsam mit seinen Partnern Microsoft, Südwestmetall, Impact AI sowie der KI-Allianz Baden-Württemberg mit dem GenAI Event KI.CKSTART eine Bildungsoffensive gestartet. Ziel der Veranstaltung war es, möglichst viele Menschen für Künstliche Intelligenz (KI) zu begeistern und Unternehmen beim Einsatz von KI zu unterstützen. Dazu kamen zahlreiche Expert_innen, Interessierte und Branchenvertreter_innen zusammen, um sich aktiv über die neusten Entwicklungen im Bereich der generativen KI auszutauschen. Unter Generativer Künstlicher Intelligenz (kurz GenAI) kann eine spezielle Art von KI-Systemen verstanden werden, die in der Lage sind, neue Inhalte in Form von beispielsweise Texten, Bildern, Videos oder sogar Programmcodes zu erzeugen. Auch große Sprachmodelle (sog. Large Language Models – LLM) basieren regelmäßig auf generativen KI-Modellen, um neue Inhalte generieren und mit den Nutzenden interagieren zu können.

Wir waren ebenfalls bei dem GenAI Event KI.CKSTART in den Stuttgarter Wagenhallen vertreten und nutzten dabei die Gelegenheit, an beiden Veranstaltungstagen vor insgesamt rund 700 Teilnehmenden einen Vortrag zum Thema „KI in der Datenschutzpraxis“ zu halten.

Im Fokus des Vortrags standen aktuelle datenschutzrechtliche Aspekte beim Einsatz Künstlicher Intelligenz im Unternehmen. Ziel war es, den Teilnehmenden konkrete und umsetzbare Hilfestellungen im Umgang mit datenverarbeitenden KI-Systemen zu bieten. Gleichzeitig präsentierten wir mit der Vorstellung unseres aktuellen Diskussionspapiers und der Orientierungshilfe KI & Datenschutz (ONKIDA) unsere Arbeit. Neben dem Vortrag war die Veranstaltung eine wichtige Plattform für den Austausch mit zentralen Akteuren der KI-Branche, um so Kontakte knüpfen und gemeinsam an der Stärkung des KI-Standorts Baden-Württemberg arbeiten zu können. Datenschutz wurde dabei nicht als Hindernis für Innovation, sondern vielmehr aktiv als Enabler für den verantwortungsvollen Einsatz von KI-Systemen positioniert, der das Vertrauen in innovative Technologien stärkt. Die Thematik Datenschutz und KI nimmt damit für die erfolgreiche digitale Transformation eine entscheidende Rolle ein. Wir werden auch künftig versuchen, eng mit Vertreter_innen aus Wirtschaft, Wissenschaft und Politik zusammenzuarbeiten, um den verantwortungsvollen Einsatz von KI voranzutreiben und Innovation aktiv zu stärken.

Online-Angebot und digitale Kommunikation

✎ Art. 57 Abs. 1 b), d), i) DS-GVO

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

Direkte Kommunikation mit Mastodon und PeerTube

Wir schätzen die direkte Kommunikation und unterstüzen dies mit einem eigenen Mastodon-Server. Auf diesem können öffentliche Stellen in Baden-Württemberg und Stellen mit Bezug zu öffentlichen Aufgaben einen Account einrichten. Über 145 Accounts sind auf dem Server eingerichtet, rund 100 Accounts sind regelmäßig aktiv. Wir nutzen unsere Accounts, um auf aktuelle Datenschutzthemen einzugehen und über unsere Themen und Veranstaltungen zu informieren. Wir berichten von unserer Arbeit und suchen den Austausch. Der LfDI-Accounts hat rund 7.000 Follower, der LfDI-Pressestellenaccount knapp über 1.250 Follower. Die Zahlen entsprechen denen des Vorjahrs.

Zuletzt haben sich eine Vielzahl von Hochschulen dafür entschieden, intensiver auf Mastodon aktiv zu sein. Auf unserem Server sind mittlerweile 50 Hochschul- und Wissenschaftsaccounts eingerichtet. Zahlreiche Ministerien und Behörden haben ebenfalls einen Account. Die Landesregierung hat frühzeitig schon im Jahr 2020 auf Mastodon einen Account eingerichtet und ist 2022 auf die LfDI-Ins-

tanz umgezogen. Im Herbst 2024 hat die Polizei Baden-Württemberg einen Account eingerichtet und informiert die Bürgerschaft über ihre Themen. Im Vergleich zum Vorjahr haben sich zahlreiche weitere Einrichtungen für einen Account auf unserem Server entschieden.

Dieser Microbloggingdienst ist Teil des Fediverses. Weiterhin ist nicht klar, ob Mastodon etwa eine tatsächliche Alternative für die gewinnorientierten Plattformen der großen Technikkonzerne sein kann. Wir haben in unserer Arbeit festgestellt, dass im Vergleich zum Vorjahr etwas mehr Diskussionsfreude zu erkennen war, auch scheint Mastodon mitunter insoweit attraktiver geworden zu sein, als dass auch Accounts, die kein Interesse an einer freundlichen Kommunikation haben, hier mittlerweile aktiver zu sein scheinen. Wir müssen davon ausgehen, dass je größer und beliebter Mastodon wird, auch kritischer und mitunter härter diskutiert wird. Durch die dezentrale Organisation von Mastodon und das Fehlen eines Algorithmus-Bestimmers aber ist davon auszugehen, dass es vermutlich wirksamer möglich ist, Hassrede weniger bedeutsam sein zu lassen.

Für uns ist Mastodon bislang sehr positiv zu bewerten. Wir freuen uns darüber, dass immer mehr Menschen und öffentliche Stellen alternative Kommunikationsorte für sich entdecken und diese nutzen. Weiterhin bieten wir baden-württembergischen Stellen an, bei uns einen Mastodon-Account einzurichten.

© Illustration: Y. Dwiputri

Folgen Sie uns auf Mastodon und PeerTube

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

mastodon

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

PeerTube

tube.bawü.social/a/lfdi_pressestelle

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

Videoplattform PeerTube

Die Videoplattform PeerTube nutzen wir selbst, können den Server derzeit aber nicht öffnen für andere öffentliche Stellen. PeerTube ist wie YouTube eine Plattform, auf der Videos zur Verfügung gestellt werden können, und Teil des Fediverse. Wir streamen live Veranstaltungen und stellen Aufzeichnungen zur Verfügung. Wir sind sehr zufrieden damit, dass wir Bewegtbild-Content datenschutzfreundlich anbieten können. Die Resonanz ist sehr erfreulich.

Um Erfahrungen zu sammeln, wie eine Öffnung des PeerTube Servers für öffentliche Stellen funktionieren kann, haben wir mit der Landeszentrale für politische Bildung Baden-Württemberg (LpB) einen Testlauf gestartet. Die ersten Erfahrungen sind sehr gut. Das Projekt der LpB, das PeerTube im Piloten genutzt hat, gab uns überwiegend positive Rückmeldungen, was Einstellungsmöglichkeiten und Nutzbarkeit betraf. PeerTube bekommt regelmäßig neue Features; war es etwa vor einigen Jahren nicht möglich, Kapitel zu setzen, so kann man heute die Videos einfach strukturieren. Die Rückmeldung aus dem Projekt war schließlich auch, was vermutlich die meisten sagen würden: Für junge Menschen ist PeerTube noch nicht so intuitiv und vertraut nutzbar wie große gewinnorientierte und sehr bekannte Anbieter. Hier können wir nicht widersprechen und sehen dies eher als einen Hinweis darauf, dass es notwendig ist, gerade auch junge Menschen nicht nur zur Anwendung von Techniken heranzuführen, sondern ihnen auch mehr Wissen zu den Technologien zu vermitteln, die sie nutzen. Wir arbeiten an der Wissensvermittlung. Die LpB macht dies in großem Umfang in ihrem Aufgabenbereich – und zeigt mit dem Testlauf, dass es auch mit einer datenschutzfreundlichen Videoplattform möglich wäre.

Internetangebot

Unser Internetangebot erfreut sich weiterhin großer Beliebtheit. Die Seite etwa mit dem von uns erstellten Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“ wurde seit Erstellung im November 2023 schätzungsweise knapp 40.000 Mal aufgerufen. Im Jahr 2024 wurden unsere Tracking FAQ über 10.000 Mal aufgerufen, unsere FAQ Hinweisgeberschutzgesetz knapp 10.000 Mal. Die Seite der KI-Woche wurde knapp 6.000 Mal aufgerufen, die mit der unserem Orientierungshilfen-Navigator 2.500 Mal. Zuletzt haben wir unsere FAQ zu Deceptive Design Patterns veröffentlicht, in denen wir über irreführende Design informieren und Hinweise geben, wie solche Designs vermieden werden können. Dabei beziehen wir uns auf die europäischen Leitlinien zu Deceptive Design Patterns – die wir in der europäischen Zusammenarbeit federführend erstellt haben.

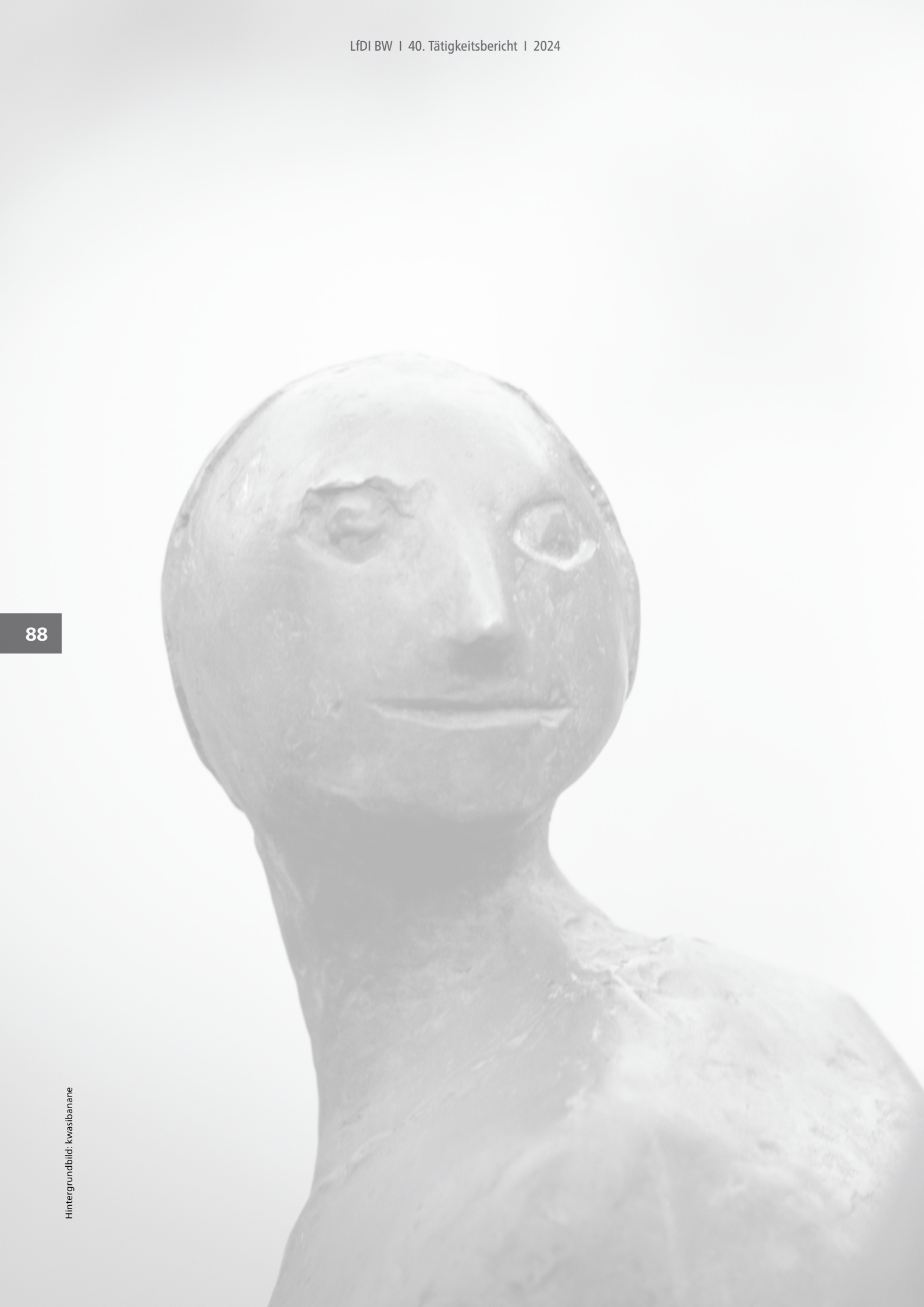
Wir haben im Jahr 2024 den Schwerpunkt auf Wissen zu KI gelegt, dieses Wissen wird rege abgerufen. Die Öffentlichkeitsarbeit sorgt dafür, dass die Fachlichkeit des Hauses möglichst viele Menschen erreicht. Wir gehen davon aus, dass durch diese Art der Wissenslieferung manche Beratungsanfrage uns erst gar nicht erreicht. Auch hoffen wir, dass verantwortliche Stellen durch die Würdigung der Inhalte ihre Anwendungen und Angebote datenschutzfreundlicher anbieten und wir wirksam dabei helfen können, Datenschutzverstöße zu vermeiden.

Podcast Datenfreiheit

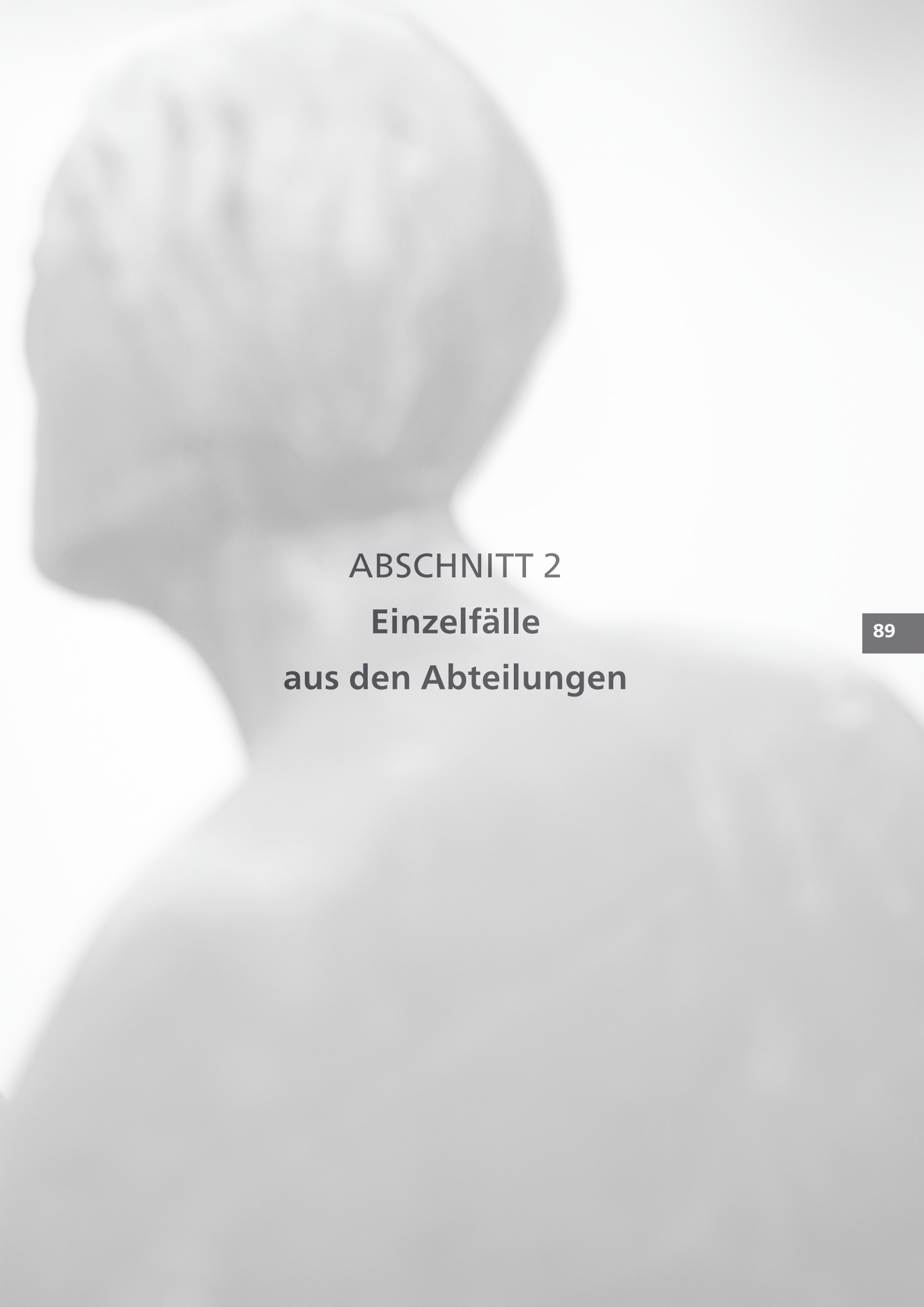
Unser Podcast Datenfreiheit hat sich als Format etabliert. Bis zu 2.500 Aufrufe einzelner Folgen zeigen uns, dass wir weiter podcasten sollten sinnvoll ist. Wir haben den Podcast zudem erweitert: Wir produzieren Extra-Folgen, in denen wir ein Thema ausführlicher diskutieren. Wir holen uns auch Gäste in Haus. Wir haben vier Folgen zum Thema KI und Bildung aufgezeichnet und diskutieren in weiteren Extra-Folgen für ein eher akademisches Publikum aktuelle Datenschutz- und KI-Themen aus der Rechtsprechung, Gesetzgebung sowie interessante Veröffentlichungen und Veranstaltungen.

☛ **Weitere Informationen**

tube.bawü.social/c/lfdi_audio/videos



Hintergrundbild: kwasibanane



ABSCHNITT 2
Einzelfälle aus den Abteilungen

© kwasibanane

Die Verwaltungseinheit des LfDI sorgt für eine stets leistungsfähige Dienststelle.

Abteilung 1: Einblick in die Dienststelle

Personalbereich

Zu Beginn des Berichtsjahres konnten einige Monate lang unbesetzte Abteilungsleitungsstellen nachbesetzt werden: Zum 15. Januar wurde die Leitung der Abteilung 2, die für die Themen Innere Sicherheit, Kommunal- und Finanzwesen, die Rechtsberatung, Angelegenheiten im Verkehr und die Videoüberwachung zuständig ist, neu besetzt. Einen Monat später folgte die Nachbesetzung der Leitung der Abteilung 1, die als Querschnittsabteilung die zentralen Servicebereiche „Organisation und IuK", „Personal" und „Finanzen" umfasst.

Der bereits in den vergangenen Jahren erfolgreiche praktizierte Personalaustausch mit anderen Landesbehörden wurde auch im Jahr 2024 fortgeführt. Es erfolgten Abordnungen aus unserem Geschäftsbereich an das Staatsministerium und an die Universität Tübingen. Dankbar sind wir für die Abordnungen aus den Geschäftsbereichen des Kultusministeriums und des Innenministeriums, mit der unsere Arbeit eine wertvolle Unterstützung erfahren hat.

Neue Einblicke brachte uns auch das Landesarchiv in Gestalt einer Referendarin im höheren Archivdienst, die für zwei Wochen bei uns war, sowie die Referendarinnen und Referendare im juristischen Bereich, die bei uns ihre mehrmonatigen Stationen ableisten.

Im Juli 2024 wurde auch ein neuer Personalrat gewählt. Wir freuen uns auf eine Fortsetzung der guten und vertrauensvollen Zusammenarbeit mit der neuen Interessenvertretung, die auch die Zusammenarbeit mit der Beauftragten für Chancengleichheit prägt.

Organisation

Im Mai 2024 jährte sich der Rollout der E-Akte zum ersten Mal. Seit dem 22. Mai 2023 führen wir alle

neuen Vorgänge nur noch in digitaler Form. Vorgänge, welcher vor diesem Stichtag noch auf Papier begonnen worden waren, führen wir ebenfalls nur noch digital weiter. Um die Umstellung möglichst effizient zu gestalten, digitalisieren wir keine Fallakten nachträglich. Diese sogenannten „Hybridakten" – also Akten, die zum Teil noch auf Papier, zum Teil digital geführt werden – sowie der noch vorhandene Papieraktenbestand aus den vorangegangenen Jahren führen dazu, dass wir die jährliche Aktenaussonderung noch wie gewohnt durchführen. Um ab dem 1. Januar 2027 auch die rein elektronische Aussonderung durchführen zu können, haben wir im Herbst das hierfür konzipierte Aussonderungsmodul ausgerollt, sodass wir einerseits die elektronischen Akten an das Landesarchiv Baden-Württemberg übergeben, andererseits Akten endgültig löschen können, deren Aufbewahrungsfrist abgelaufen ist. Die E-Akte ist inzwischen in unserer Behörde etabliert und neue Funktionalitäten, wie der sichere Übermittlungsweg von Schriftgut über das besondere Behördenpostfach (beBPo), steigern die Effizienz der täglichen Arbeit.

Unsere Diensträume in der Lautenschlagerstraße 20 im Herzen von Stuttgart haben sich seit dem Umzug im Jahr 2021 für unsere Ziel- und Aufgabenerfüllung bewährt. Besonders die Seminarräume unseres Bildungszentrums Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB) mit ihrer zeitgemäßen technischen Ausstattung haben es uns erlaubt, den Informations-, Schulungs- und Beratungsauftrag unserer Behörde unter Zuhilfenahme moderner Medienformate zu erfüllen. Wir bedauern es deshalb, die Diensträume wieder verlassen zu müssen. Der Vermieter plant eine Neubebauung des Grundstücks ab dem Jahr 2026. Mit Vermögen und Bau – Amt Stuttgart haben wir deshalb bereits im Berichtsjahr den Suchprozess nach neuen und geeigneten Diensträumlichkeiten gestartet. Unser Ziel ist ein Umzug im dritten Quartal 2025, damit Baden-Württemberg turnusgemäß im Jahr 2026 den Vorsitz der Datenschutzkonferenz aller bundesdeutschen Aufsichtsbehörden übernehmen und die damit verbundenen Veranstaltungen am neuen Standort durchführen kann.

Die bisherige Bußgeldstelle im Hause wurde zum 1. August 2024 in zwei Einheiten aufgeteilt: Die Bußgeldstelle Digitale Dienste soll den Fokus auf Verfahren nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) richten, während die Allgemeine Bußgeldstelle Verstöße gegen sonstige bußgeldbewehrte Normen im Datenschutzrecht verfolgt.

Finanzen

In der Bücherei der Dienststelle, die beim Sachgebiet Finanzen angesiedelt ist, wurden im Jahr 2024 die Zeitschriften und Loseblattsammlung zu einem großen Teil auf digitale Angebote umgestellt. Somit stehen unseren Bediensteten moderne Recherchemöglichkeit zur juristischen Fallbearbeitung zur Verfügung.

Im Finanzbereich war das Jahr 2024 von der Aufstellung des Staatshaushaltsplans 2025 / 2026 für den Geschäftsbereich des LfDI (Einzelplan 17) geprägt. Die Eingabe der Daten erfolgte zum ersten Mal im neuen SAP-Haushaltsmanagementsystem PH2. Dabei mussten einige technische Hürden überwunden werden, um alle Daten fristgerecht dem für die Planaufstellung federführenden Finanzministerium übergeben zu können.

Im Haushalt 2025 / 2026 konnten die erforderlichen Umzugskosten und eine zur tarifkonformen Eingruppierung notwendige Stellenhebung berücksichtigt werden. Bei drei an das Projekt „SchuleDigital" gebundene Referentenstellen mussten zum 1. Januar 2025 „künftig wegfallend (kw)-Vermerke" vollzogen werden, sodass diese Stellen entfallen.

© Illustration: Y. Dwiputri

Beauftragte für Chancengleichheit

Das Chancengleichheitsgesetz gilt in Baden-Württemberg seit 2016. Mit dem neuen „Gesetz zur Verwirklichung der Chancengleichheit von Frauen und Männern im öffentlichen Dienst in Baden-Württemberg“ will die Landesregierung das berufliche Vorankommen von Frauen in der Verwaltung gezielt fördern und die Vereinbarkeit von Familie, Pflege und Beruf verbessern.

Generelle Zuständigkeiten der Beauftragten für Chancengleichheit (BfC) beinhalten z. B.:

- Einhaltung und Durchführung des Chancengleichheitsgesetzes
- Förderung von Maßnahmen zur Vereinbarkeit von Familie, Pflege und Beruf

Dies umfasst z. B. die Beteiligung bei allgemeinen personellen sowie sozialen und organisatorischen Maßnahmen der Dienststelle. Die BfC ist der Dienststellenleitung unmittelbar zugeordnet und hat ein unmittelbares Vortragsrecht (§ 18 ChancenG). Somit ist die BfC keine Interessensvertretung, in der Ausübung ihrer Tätigkeit unabhängig und nicht an Weisungen gebunden.

Beim LfDI fand die erste Chancengleichheitswahl im Jahr 2018 statt (siehe 34. Tätigkeitsbericht 2018, S. 127), seitdem haben einige engagierte Mitarbeiterinnen das Amt ausgeübt. Im Berichtsjahr begann für zwei Kolleginnen die neue Amtszeit.

BfC-Leseecke

Seit einigen Jahren bildet eine sorgfältig ausgewählte Sammlung an Büchern zu z. B. Chancengleichheit, Empowerment und Persönlichkeitsentwicklung eine BfC-Leseecke innerhalb des Hauses. Mit einer bunten Mischung von inspirierenden Biografien, Romanen und Sachbüchern lädt sie unter anderem dazu ein, in Geschichten starker Frauen und Autorinnen einzutauchen, die Mut und Durchsetzungsvermögen vermitteln. Ziel des Angebots ist, alle Interessierten literarisch weiterzubilden und sich mit den facettenreichen Themen spielerisch auseinanderzusetzen.

BfCafé

Um ein Gefühl für die Wünsche und Bedürfnisse des Hauses zu bekommen, wurde das BfCafé ins Leben gerufen. Zweimal jährlich wird hierzu die gesamte Dienststelle eingeladen, sich bei einem Kaffee auszutauschen. Hier ist es in lockerer Atmosphäre möglich, unter anderem mit der BfC selbst über persönliche Wünsche in Bezug zur Chancengleichheit, Familie, Pflege etc. zu sprechen. Hierbei wurde der Blick der BfC für die Themen geschärft, die für die Mitarbeitenden wichtig sind. Auch positive Entwicklungen und Feedback zu Veranstaltungen konnten so besser erfasst werden. Der niederschwellige Austausch kam beim Kollegium sehr gut an und wird nachgefragt. Wir konnten verzeichnen, dass sich viel mehr Menschen beim Informationssammeln und Verbreiten beteiligen und generell offener und interessierter an der Arbeit der BfC sind.

Workshop

Außerdem hat die BfC im Zuge ihrer Tätigkeiten zwei Workshops organisiert, die jeweils die Abteilungsleitungen und die Mitarbeitenden gesondert adressiert und sensibilisiert haben. Mit mehr als der Hälfte der Belegschaft verzeichneten beide Veranstaltungen sehr hohe Anmeldezahlen. Die BfC erhielt positive Rückmeldungen zu Inhalt, Format und Referentin.

Auch für das nächste Jahr sollen Wünsche aus dem Kollegium für Themenschwerpunkte oder Veranstaltungen stark im Fokus stehen. Ziel der BfC ist, das Vertrauen und die starke Beteiligung aus dem Kollegium weiter zu fördern. Die positive Resonanz soll die treibende Kraft der BfC bleiben.

Abteilung 2: Inneres, Videoüberwachung und Verkehr

Wissen vernetzen: datenschutzrechtliche Beratung für öffentliche Stellen

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

Wie in den vergangenen Jahren haben wir auch in diesem Jahr proaktiv nach Wegen gesucht, öffentliche Stellen bei der Vielzahl ihrer Aufgaben, bei welchen sie personenbezogene Daten verarbeiten, zu unterstützen.

Referentinnen unseres Hauses haben in der ersten Jahreshälfte an verschiedenen Arbeitskreisen teilgenommen, unter anderem des Landkreistages, des Städtetages und des Kommunalen Netzwerks Datenschutz der Kehler Akademie e.V. Hierbei haben wir uns mit den Teilnehmenden über zahlreiche aktuelle datenschutzrechtliche Fragestellungen ausgetauscht.

Erneut fand das Forum kommunaler Datenschutz in unseren Räumlichkeiten statt. Beim Forum kommunaler Datenschutz handelt es sich um ein von uns in wechselnder Besetzung veranstaltetes Expertengremium, in dem die kommunalen Interessensverbände und Praktiker_innen sich mit uns über konkrete datenschutzrechtliche Fragen austauschen können. Zuvor haben wir über unsere Website alle öffentlichen Stellen in Baden-Württemberg dazu aufgerufen, Fragen bei uns einzureichen. Die eingereichten Fragen wurden sodann im Expertengremium diskutiert und im Anschluss auf unserer Website veröffentlicht.

Die Schulung „Datenschutzgrundlagen für öffentliche Stellen“ wurde auch in diesem Jahr mehrfach durchgeführt, nach wie vor mit großer Resonanz. Im Rahmen der Schulung kommen wir regelmäßig mit den Mitarbeitenden öffentlicher Stellen und deren aktuellen datenschutzrechtlichen Fragestellungen in Kontakt.

Ebenso erreichten uns zahlreiche schriftliche und telefonische Beratungsanfragen von öffentlichen Stellen zu den unterschiedlichsten datenschutzrechtlichen Fragestellungen.

Wir veröffentlichen auch pro aktiv Informationen auf unserer Website, insbesondere, wenn uns zu bestimmten, aktuellen Fragestellungen vermehrt Anfragen oder Beschwerden erreichen. So standen sowohl bei den öffentlichen Stellen als auch bei vielen Bürger_innen in der ersten Hälfte dieses Jahres die Kommunalwahlen im Fokus. Dies haben wir zum Anlass genommen, eine aktuelle Zusammenstellung von Fundstellen zu veröffentlichen, die viele wichtige Fragen rund um die Kommunalwahlen und die Arbeit der Gemeinderäte. adressieren. Ein weiterer „Dauerbrenner“ sind Fragen und Beschwerden von Bürger_innen – aber auch von den öffentlichen Stellen selbst – zu dem Themenkomplex der Weitergabe von Adressdaten durch die Meldebehörden. Auch hierauf sind wir eingegangen und haben die „FAQ Datenweitergabe durch Meldebehörden“ auf unserer Website veröffentlicht. Eine weitere aktuelle Veröffentlichung umfasst „Tipps für Kommunen, die Mängelmelder nutzen (wollen)“, da auch hierbei, sofern personenbezogenen Daten verarbeitet werden, datenschutzrechtliche Vorschriften zu beachten sind.

Durch die vielfältigen Einblicke in die Arbeit der öffentlichen Stellen, welche wir auch in diesem Jahr erhalten haben, und den Austausch auf unterschiedlichen Ebenen und mit verschiedenen Akteuren, stellen wir immer mehr fest, wie enorm wichtig eine gute Vernetzung der öffentlichen Stellen untereinander ist, um ein effektives Wissensmanagement voranzubringen. Denn häufig sind die Stellen mit denselben datenschutzrechtlichen Fragen konfrontiert und könnten von einem Austausch untereinander enorm profitieren. Teilweise gibt es schon etablierte Formate, in denen auch ein Wissensmanagement beinhaltet ist, allerdings sind noch längst nicht alle öffentliche Stellen in Baden-Württemberg an einem solchen Austausch beteiligt. Aus unserer

Sicht würde der Ausbau der Vernetzung und der stetige Austausch von bereits vorhandenem Wissen zu datenschutzrechtlichen Fragestellungen zu einer Entlastung der einzelnen Stellen führen und insgesamt zu einer Verbesserung des Datenschutzes.

☛ Weitere Informationen

Kommunalwahlen in Baden-Württemberg:
www.baden-wuerttemberg.datenschutz.de/kommunalwahlen-bw-2024

FAQ Datenweitergabe durch Meldebehörden:
www.baden-wuerttemberg.datenschutz.de/faq-datenweitergabe-durch-meldebehoerden

Tipps für Kommunen, die Mängelmelder nutzen (wollen):
www.baden-wuerttemberg.datenschutz.de/tipps-fuer-kommunen-die-maengelmelder-nutzen-wollen

FAQ Kommunaler Datenschutz:
www.baden-wuerttemberg.datenschutz.de/faq-kommunaler-datenschutz

Überwachte Mieter_innen im Investoren-Objekt

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

In Zeiten von Wohnraummangel und Investorengeschäften im Bereich Wohnbau und Sanierung scheint die Luft für Mieter_innen auch in Sachen Datenschutz zunehmend dünner zu werden. Eine bei uns eingereichte Beschwerde richtete sich gegen eine weiträumige Videoüberwachung einer großen Wohnanlage, andernorts sollten Kameras in einem Treppenhaus Beweise im Rahmen eines Räumungsprozesses liefern. Letzterem schob der Bundesgerichtshof einen Riegel vor.

Überwachung im Investoren-Objekt

Die bei uns eingereichte Beschwerde richtete sich gegen die Hausverwaltung einer Wohnanlage mit ca. 90 Einheiten, die von einem regionalen Investor vermietet wird. Laut des Beschwerdeführers habe der Investor ihn als Mieter bereits in der Vergangenheit im Stich gelassen, beispielsweise indem er sich vor erforderlichen Reparaturen an der Heizung gedrückt habe und erst in letzter Minute vor einem bereits anberaumten Gerichtstermin einlenkte. Gleichwohl sei er über den neuerlichen Hinweis, dass sämtliche Flure, die Waschküche, der Ausgang zur Dachterrasse und der Eingangsbereich videoüberwacht werden sollten, überrascht gewesen. Während die Hausverwaltung in einem Anschreiben an die Mieter_innen die Videoüberwachung zunächst noch damit begründete, dass „die Brandquelle in einem Brandfall umgehend identifiziert und entsprechend bekämpft werden kann“, trug sie uns gegenüber vor, dass es zu „wiederholte[n] Vorfälle[n] von körperlichen Auseinandersetzungen und Eigentumsverletzungen“ gekommen sei, wofür jedoch weder Nachweise oder Dokumentationen vorgelegt, noch die angeblich entstandenen Schäden beziffert wurden. Selbst bei Vorliegen entsprechender Nachweise wäre die Zulässigkeit der Videoüberwachung jedoch fraglich gewesen. Die Bedingung der Rechtsgrundlage in Art. 6 Abs. 1 Buchst. f) DS-GVO lautet: Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, 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.

Eine Prüfung milderer Mittel wurde nicht im ausreichenden Umfang vorgelegt. Dem Vortrag, dass sich der Versuch, den Schutz von Mietern und Mietobjekt durch die Präsenz des Hausmeisters sicherzustellen, als unzureichend erwiesen habe und der Vorgänger des aktuellen Hausmeisters selbst schon Opfer einer tätlichen Auseinandersetzung geworden sei, fehlt es bereits an Angaben zur zeitlichen und räumlichen Einordnung. Auch die Ergänzung, dass Alarmanlagen aufgrund des Umstandes, dass es sich bei den Bereichen, in denen sich die Vorfälle abgespielt hätten, um allgemein zugängliche Räume handelt, keine adäquate Lösung seien, reicht zur Begründung der Erforderlichkeit nicht aus. Eine Prüfung weiterer Möglichkeiten wie z. B. eine verstärkte Beleuchtung, Einsatz von Brandmeldern, Verzicht auf eine gemeinsame Waschküche und Entsorgungsmöglichkeiten für den Fluchtwege einschränkenden Sperrmüll wurden nicht vorgetragen.

Nicht nur in der Wohnung, sondern auch im Treppenhaus sollten keine rechtswidrigen Kameraüberwachungen stattfinden.

Im Übrigen dürften hier die Interessen der betroffenen Mieter_innen überwiegen. Aufgrund der Nähe zur Wohnung als privaten Rückzugsort ist der Eingriff als intensiv zu bewerten. In dieser Situation haben die Mieter_innen auch nicht mit einer Überwachung zu rechnen. Das Mietverhältnis begründet eine Abhängigkeit unter einem Machtgefälle. Demgegenüber bleiben die für den Investor entstandenen Schäden nur vage. Unsere Bewertung nahm die Hausverwaltung zum Anlass, die Videoüberwachung zu beenden.

Bundesgerichtshof lässt Verwertung von Kameraaufnahmen nicht zu

Im Rahmen eines Räumungsklage-Prozesses wegen angeblich unzulässiger Untervermietung hat der Bundesgerichtshof (BGH) die Verwertung der Erkenntnisse aus einer heimlichen Videoaufzeichnungen als unzulässig bewertet. Eine Privatdetektivin hatte mittels im Treppenhaus angebrachter Kameras heimlich den bei geöffneter Wohnungstür erfassten Eingangsbereich innerhalb der Wohnungen überwacht, die Aufnahmen gespeichert und ein Protokoll darüber erstellt, wann welche Personen ein- und ausgegangen waren. Laut des BGH verletze die Videoüberwachung das Recht der Mieter_innen auf Unverletzlichkeit der Wohnung (Art. 13 I GG) und ihr allgemeines Persönlichkeitsrecht in der Ausprägung als Recht auf informationelle Selbstbestimmung (Art. 2 I GG, Art. 1 I GG) (BGH, Urt. v. 12.3.2024, Az. VI ZR 1370 / 20).

Anders als in dem viel diskutierten Urteil des BGH, in welchem er die Verwertung datenschutzwidrig erhobener Dashcam-Aufnahmen dennoch als Beweismittel in einem Unfallhaftpflichtprozess zugelassen hatte (BGH, Urt. v. 15.05.2018 – VI ZR 233 / 17), durften die unzulässigen Aufnahmen im vorliegenden Fall nicht als Beweismittel verwertet werden. Nach

der ständigen Rechtsprechung führt die Unzulässigkeit oder Rechtswidrigkeit einer Beweiserhebung nicht ohne Weiteres zu einem Beweisverwertungsverbot (BGH ebenda mit Verweis auf BVerfG, Beschl. v. 9. 11. 2010 – 2 BvR 2101 / 09 Rn. 45; BVerfG, Beschl. v. 20. 5. 2011 – 2 BvR 2072 / 10, Rn. 12 jew. mwN). Ob ein Eingriff in das allgemeine Persönlichkeitsrecht des Beweisgegners durch die Verwertung von Beweismitteln gerechtfertigt ist, richtet sich nach dem Ergebnis der Abwägung zwischen dem gegen die Verwertung streitenden allgemeinen Persönlichkeitsrecht, hier in seiner Ausprägung als Recht auf informationelle Selbstbestimmung, auf der einen und den für die Verwertung sprechenden rechtlich geschützten Interessen auf der anderen Seite (BGH ebenda m. Verw. auf BVerfG, Beschluss vom 9. 10. 2002 – 1 BvR 1611 / 96, 1 BvR 805 / 98).

Dem BGH zufolge mussten die betroffenen Mieter_innen unter den konkreten Umständen vernünftigerweise nicht mit der Erhebung und Verarbeitung der personenbezogenen Daten rechnen. Ihnen war die Möglichkeit genommen, ihr in der räumlichen Privatsphäre gezeigtes Verhalten an die Beobachtung anzupassen. Sie hatten auch keine Möglichkeit, auf den vorhandenen Datenbestand einzuwirken. Demgegenüber war die andere Seite keiner Beweisnot ausgesetzt, da ihr mildere Mittel zum Nachweis etwaig anhaltender Gebrauchsüberlassungen zur Verfügung standen, wie z. B. eine sog. Scheinanmietung.

Wird auf Mieter_innen mittels Videoüberwachung rechtswidrig Druck ausgeübt, muss neben einer Untersagung der Videoüberwachung auch mit einem Bußgeld gerechnet werden. Dass eine Videoüberwachung im Bereich des Wohnraums von ganz anderer Qualität als im öffentlichen Straßenraum ist, zeigt nicht zuletzt das Urteil des Bundesgerichtshofs.

Ruhe in Unfrieden – Videoüberwachung auf dem Friedhof

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

Grabschmuck, den Angehörige an der letzten Ruhestätte eines Verstorbenen angebracht haben, ziert nun einen fremden Balkonkasten. In einer anderen Gemeinde werden Brandspuren auf einem Grab festgestellt und eine Grablaterne verschwindet. Während die Toten sich derartiges wohl oder übel gefallen lassen müssen, erwägen Gemeinden und Nutzungsberechtigte von Gräbern, eine Videoüberwachungsanlage einzusetzen. Wir haben hierzu beraten und verhängten ein Bußgeld.

Für Nutzungsberechtigte von Gräbern, zumeist Angehörige der Verstorbenen, ist als Rechtsgrundlage für eine Videoüberwachung lediglich Art. 6 Abs. 1 Buchst. f) DS-GVO praktisch relevant. Danach ist die Verarbeitung zulässig, wenn folgende Bedingungen erfüllt sind: die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (1) erforderlich (2), 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 (3). Ein berechtigtes Interesse der Nutzungsberechtigten des Grabes kann beispielsweise in der Sicherung von Beweisen im Falle von Beschädigung und Schändung des Grabes oder Diebstahl zu sehen sein. Die Vorfälle müssten gem. Art. 5 Abs. 2 DS-GVO nachweisbar bzw. dokumentiert sein. Im Hinblick auf die Erforderlichkeit kann eine nur auf die Grabanlage beschränkte Überwachung bereits daran scheitern, dass die in einem so kleinräumigen Überwachungsbereich erzeugten Aufzeichnungen als Beweismittel ungeeignet wären. Etwaige im Einzelfall zur Verfügung stehenden milderen Mittel als die Videoüberwachung sind zu prüfen. Reicht ein im Übrigen erforderlicher Überwachungsbereich über das Grab selbst hinaus, ist zu beachten, dass weitere Personen von der Videoüberwachung betroffen sein können.

Dann muss im Rahmen der Interessenabwägung der Besonderheit des Ortes Rechnung getragen werden. Friedhöfe werden gemeinhin als Orte des ehrenden Gedenkens und der Ruhe aber auch der Begegnung wahrgenommen. Dabei ist zu beachten, dass bei Trauerfeiern und beim Aufsuchen von Gräbern häufig religiösen und weltanschaulichen Überzeugungen Ausdruck verliehen wird. In die-

sem Kontext dürfen die betroffenen Personen davon ausgehen, dass auf ein damit verbundenes Bedürfnis nach Ungestörtheit Rücksicht genommen wird. Sie haben daher nicht damit zu rechnen, dass eine Videoüberwachung stattfindet. Der Informationsgehalt von etwaig angefertigten Aufnahmen kann u. U. relativ hoch sein und Informationen zum Gegenstand haben, die in Anlehnung an die von der Rechtsprechung zum Allgemeinen Persönlichkeitsrecht geprägte sog. Sphärentheorie der Privatsphäre zuzuordnen sind. Der Schutz der Privatsphäre gem. Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK umfasst insbesondere Angelegenheiten, die wegen ihres Informationsgehalts typischerweise als „privat" eingestuft werden. Dazu können auch Situationen großer emotionaler Belastung wie bei der Trauer um einen Angehörigen oder eine nahestehende Person zählen. Diese können Gefühlsäußerungen, persönliche Regungen und Handlungen auslösen, die erkennbar nicht für die Augen Dritter bzw. Unbeteiligter bestimmt sind (vgl. BGH, Urteil vom 10.11.2020 – VI ZR 62 / 17 – KG Rnn. 15 ff. m. w. N.). Zu denken ist beispielsweise an tröstender Gesten gegenüber Trauernden.

Auch wenn ein Friedhof öffentlich zugänglich ist, kann daraus nicht ohne Weiteres geschlossen werden, dass betroffene Personen nicht die berechtigte Erwartung haben, in Ruhe gelassen zu werden. Der Schutzbereich der Privatsphäre ist nicht nur örtlich, sondern auch thematisch bestimmt (vgl. BGH Urt. v. 13.12.2022 – VI ZR 280 / 21 Rn. 35). Dabei ist zu beachten, dass private Bestattungsplätze nach § 9 des Bestattungsgesetzes nur in engen Grenzen angelegt werden dürfen („Friedhofszwang"). Für Hinterbliebene besteht daher in vielen Fällen zur Nutzung des gemeindlichen Friedhofs keine zumutbare Alternative. Daher kann beispielsweise die Aufschrift des Bandes eines Grabkranzes, den Eltern am Grab ihres verstorbenen Sohnes niedergelegt haben, deren Privatsphäre zugeordnet werden (BGH, Urteil vom 10.11.2020 – VI ZR 62 / 17 – KG Rn. 17).

Von Seiten der Gemeinde wäre eine Videoüberwachung nur unter den engen Voraussetzungen des § 18 des Landesdatenschutzgesetzes (LDSG) zulässig. Dabei ist insbesondere die abschließende Auflistung von Schutzgütern in § 18 Abs. 1 LDSG zu beachten. Während zu den Schutzgütern des Straftatbestands der Störung der Totenruhe (§ 168 StGB) beispielsweise auch das Pietätsgefühl der Angehörigen der Verstorbenen, die mit dem Tod nicht endende Menschenwürde, das Pietätsgefühl der Allgemeinheit und der öffentliche Frieden (vgl. Heuchemer, in BeckOK StGB, 61. Edition, § 168 Rn. 1) zählen, finden sich diese in § 18 LDSG nicht wieder. Als milderes Mittel ist etwa an beschränkte Öffnungszeiten, Beleuchtung während der Nachtstunden und verstärkte Kontrollen sowie Sensibilisierungsmaßnahmen gegenüber den Einwohnern zu denken. Auf der nächsten Prüfungsebene können wiederum im Rahmen einer umfassenden Interessenabwägung seitens der Gemeinde neben individuellen Schutzgütern auch Aspekte von allgemeinem Interesse wie die Schutzgüter des § 168 StGB Berücksichtigung finden.

Der Vergleich der in Betracht kommenden Rechtsgrundlagen zeigt, dass Gemeinden und Privatpersonen nicht in jedem Fall die gleichen Handlungsmöglichkeiten zustehen. Andererseits besteht für Gemeinden auch die Möglichkeit, in einer Satzung nach § 15 des Bestattungsgesetzes Videokameras auf dem Friedhof zu verbieten. Im Rahmen der Prüfung des Art. 6 Abs. 1 Buchst. f) DS-GVO würde dies dazu führen, dass bereits kein berechtigtes Interesse an einer Datenverarbeitung vorliegen würde. Eine Prüfung sämtlicher Umstände von Einzelfällen würde sich erübrigen. Bei einem Verstoß gegen die Friedhofsordnung wegen einer unzulässiger Datenverarbeitung wären wir als Aufsichtsbehörde gemäß Art. 51 DS-GVO i.V.m. § 40 des Bundesdatenschutzgesetzes i.V.m. § 25 Abs. 1 S. 2 LDSG zuständig. Verstöße wegen des unzulässigen Anbringens von Attrappen sind demgegenüber Sache der Gemeinde.

Bezahlkarte statt Bargeld für Geflüchtete – auch ein datenschutzrechtliches Thema

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

Die sog. Bezahlkarte soll die Gewährung von Leistungen an Asylbewerber_innen vereinfachen. Dabei hat die Verwaltung viel Gestaltungsspielraum.

Allerdings müssen bei Zusatzfunktionen der Bezahlkarte datenschutzrechtliche Grenzen beachtet werden. Wir haben gemeinsam mit anderen Aufsichtsbehörden ein Positionspapier für die Datenschutzkonferenz (DSK) dazu erarbeitet sowie die Arbeitsgruppe der 14 Bundesländer beraten, die zur Einführung der Bezahlkarte ein gemeinsames Vergabeverfahren durchgeführt haben.

Am 16. März 2024 ist eine Änderung des Asylbewerberleistungsgesetzes (AsylbLG) in Kraft getreten (BGBl. 2024 I Nr. 152 vom 15.05.2024, S. 29 f.). Nunmehr dürfen Leistungen nach dem AsylbLG in verschiedenen Kontexten auch durch eine sog. Bezahlkarte gewährt werden, s. §§ 2, 3 und 11 AsylbLG. Der vorher darüber geführte Streit, ob eine Bezahlkarte auch ohne Gesetzesänderung eingeführt werden könnte, hat sich somit erledigt. Nicht erledigt ist allerdings die Auseinandersetzung mit einzelnen Funktionen der Bezahlkarte, die teilweise auch vom Datenschutzrecht begrenzt werden.

Nach Vorstellung des Gesetzgebers ist die Bezahlkarte eine guthabenbasierte Karte mit Debitfunktion (ohne Kontobindung). Sie soll als Bargeldsurrogat dienen und eine elektronische Bezahlung in Geschäften und bei Dienstleistern ermöglichen (BT-Drs. 20 / 11006, S. 101). Die Länder haben sich über diese Grundfunktion hinaus auf sog. „Mindeststandards" der Bezahlkarte geeinigt. Vorgesehen sind also über die Nutzung als Bargeldsurrogat hinausgehende Funktionen. Dabei entstehen auch datenschutzrechtliche Fragen. In dem Ansinnen, den zuständigen Leistungsbehörden einen einheitlichen datenschutzrechtlichen Rahmen zur Umsetzung der Bezahlkarte geben zu können, haben wir gemeinsam mit anderen Aufsichtsbehörden ein Positionspapier für die DSK erarbeitet. Darin werden einige der in den Mindeststandards der Länder erwünschten Funktionen aus datenschutzrechtlicher Sicht beleuchtet.

Aus Perspektive des Datenschutzes ist dabei Folgendes entscheidend: Da der Gesetzgeber die Bezahlkarte lediglich als Methode der Leistungsgewährung in §§ 2, 3 und 11 des AsylbLG eingefügt hat, handelt es sich bei dieser neuen Vorschrift nicht um eine Rechtsgrundlage im Sinne des Art. 6 Abs. 1 Abs. 1 Buchst. e DS-GVO. Die Verarbeitung personenbezogener Daten zum Zwecke der Leistungsgewährung mittels einer Bezahlkarte kann demnach nur auf die jeweiligen landesrechtlichen Generalklauseln gestützt werden, in Baden-Württemberg folglich auf § 4 LDSG. Entscheidend für die datenschutzrechtliche Zulässigkeit aller Funktionen der Bezahlkarte ist damit, dass die mit ihnen einhergehenden Verarbeitungen personenbezogener Daten für die Leistungsgewährung erforderlich sind. Soweit Funktionen für die Leistungsgewährung nicht benötigt werden, weil die Leistung schlicht ohne sie erbracht werden kann, sind die mit diesen Funktionen einhergehenden Verarbeitungsvorgänge rechtswidrig. Dies ist bei folgenden Funktionen der Fall, sie sind zur Leistungsgewährung nicht erforderlich und damit datenschutzrechtlich unzulässig:

1. Autonome Möglichkeit der Leistungsbehörden, Einsicht in den jeweiligen Guthabenstand der Leistungsberechtigten zu nehmen.

2. Pauschale Einschränkung der Nutzbarkeit der Bezahlkarte auf bestimmte Postleitzahlengebiete.

3. Automatisierter behördenübergreifender Datenabgleich von Bezahlkarteninhaber_innen außerhalb des Ausländerzentralregisters.

Für die Umsetzung der Bezahlkarte werden private Dienstleister eingebunden. Auch dabei sind datenschutzrechtliche Vorgaben zu beachten. Dazu gehört insbesondere:

1. Keine Weitergabe der Ausländerzentralregisternummer an den Bezahlkartendienstleister.

2. Trennung der Datensätze verschiedener Behörden beim gleichen Dienstleister (Mandantentrennung).

3. Kein automatisierter Abgleich aller bei einem Dienstleister gespeicherten Datensätze.

Nähere Ausführungen zu den einzelnen Punkten können dem Positionspapier der DSK entnommen werden.

Beispielhaft sei hier die Einsichtnahme in den Guthabenstand näher erläutert: Diese wäre eine Verarbeitung personenbezogener Daten der leistungsberechtigten Person durch die jeweilige Leistungsbehörde. Rechtsgrundlage dafür kann nur die o.g. datenschutzrechtliche Generalklausel sein, mithin § 4 LDSG. Die zu erfüllende Aufgabe ist die Leistungsgewährung auf Grundlage des AsylbLG. Da der Gesetzgeber nur das Mittel „Bezahlkarte" in das AsylbLG eingefügt hat, bestehen keine Anhaltspunkte dafür, dass die Aufgabenerfüllung ein Mehr an Datenverarbeitung der Leistungsberechtigten benötigt, als dies bisher der Fall war. Die Leistungsgewährung war bisher mit der Ausgabe einer Sachleistung oder eines Wertgutscheins, Gewährung einer unbaren Abrechnung oder der Auszahlung von Bargeld abgeschlossen – ebenso muss es sich demnach mit den Bezahlkarten verhalten: Die Leistungsgewährung ist mit Aushändigung der Karte, bzw. Aufladung des Guthabens erfolgt. Die selbstständige Einsichtnahme wird dafür nicht benötigt und ist stattdessen geeignet, ein Gefühl der anlasslosen und ständigen Überwachung zu vermitteln. Sollte eine Einsichtnahme im Einzelfall erforderlich sein, z. B. weil eine Karte verloren wurde und der Guthabenstand auf eine neue Karte übertragen werden muss, kann die betroffene Person auf Grundlage ihrer Mitwirkungspflicht nach § 9 Abs. 3 AsylbLG i.V.m. §§ 60 ff. SGB I dazu angehalten werden, die einmalige Einsicht in den Guthabenstand zu ermöglichen, bspw. durch ein Einloggen am Behördencomputer.

Neben dem Beschluss der DSK zur Bezahlkarte waren wir auch an einer Arbeitsgruppe mehrerer Aufsichtsbehörden beteiligt, die diejenigen 14 Länder beraten hat, welche die Bezahlkarte in einem gemeinsamen Vergabeverfahren eingeführt haben. Auch hier war das Ziel, frühzeitig unsere Expertise zur Verfügung zu stellen, um die Leistungsbehörden als verantwortliche Stellen zu entlasten.

Bei der Einführung der Bezahlkarte in das AsylbLG hat der Gesetzgeber keine Rechtsgrundlage für die damit einhergehenden Verarbeitungen personenbezogener Daten geschaffen. Damit kommt es für die Zulässigkeit der mit der Bezahlkarte einhergehenden Verarbeitungsvorgänge die Voraussetzungen der datenschutzrechtlichen Generalklauseln an. Es sind deswegen nur solche Funktionen der Bezahlkarte zulässig, deren Verarbeitung für die Leistungsgewährung selbst erforderlich sind. Zur Unterstützung einer einheitlichen Umsetzung der Bezahlkarte in den Ländern haben wir gemeinsam mit anderen Aufsichtsbehörden ein Positionspapier der DSK dazu erarbeitet sowie die Arbeitsgruppe derjenigen Länder mitberaten, die die Bezahlkarte in einem gemeinsamen Vergabeverfahren eingeführt haben.

☛ Weitere Informationen

Positionspapier Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG):
www.datenschutzkonferenz-online.de/media/dskb/2024_08_19_DSK_Beschluss_Bezahlkarte.pdf

Fußballfieber in der Schwabenmetropole

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

Im Juni sollte der Ball im Rahmen der EURO 2024 auch in Stuttgart rollen und die Ausrichter erwarteten eine Vielzahl von nationalen und internationalen Fans in der Stadt. Dabei sollte die Veranstaltung in der Innenstadt aufgrund der Gesamtlage mit umfangreicher Videotechnik begleitet werden.

Die Stadt Stuttgart wandte sich Mitte März 2024 mit datenschutzrechtlichen Fragen zu dem ihr vorgelegten Videoeinsatzkonzept zur UEFA EURO 2024 an uns. Eine eigenständige Gesellschaft der Stadt war mit der Durchführung des Public Viewing und des umfangreichen Rahmenprogramms beauftragt worden. Bereits vor unserer Einbindung wurde eine erforderliche Risikoanalyse verschiedener beteiligter Stellen erstellt, aus der sich ergab, dass aufgrund der zu erwartenden Besucherströme die Notwendigkeit bestehen könnte, während des Veranstaltungszeitraums auf und zwischen den Veranstaltungsorten in der Innenstadt – aber auch auf dem Weg zum Stadion – eine zielführende und vorausschauende Besucherlenkung vorzu-

nehmen. Dafür sollten zwischen dem 13. Juni 2024 und dem 24. Juli 2024 eine Vielzahl von Abschnitten der Stuttgarter Innenstadt (zeitweise) mittels Videokameras überwacht werden. Während definierter Zeitfenster sollten Besucherströme und auftretende Menschenbewegungen videographiert werden. Hiermit sollten einerseits Besucherströme koordiniert und gelenkt und andererseits, sich anbahnende oder stattfindende Gefahren unter anwesenden Fans erkannt und möglichst schnell geeignete Gegenmaßnahmen ergriffen und koordiniert werden.

Aus dem Entwurf des Videoeinsatzkonzepts ging hervor, dass ein Host City Operations Center (HCOC) eingerichtet werden sollte, in dem während des Veranstaltungszeitraums das höchste beschlussfassende Gremium des Ereignisses in Stuttgart seinen Sitz haben und zentral das Geschehen der gesamten Veranstaltung in der Stadt überblicken sowie steuern sollte. Zu dem beschlussfassenden Gremium sollten neben den Behörden mit Ordnungs- Sicherheitsaufgaben (BOS) auch Vertreter_innen des ÖPNV, Behörden der Stadt und Vertreter_innen des Veranstalters gehören.

So sehr wir die Intentionen der beteiligten Stellen nachvollziehen konnten, verblieben bei dem vorgelegten Konzept zahlreiche offene datenschutzrechtliche Fragen. Die Veranstalterin führte in dem Konzept an, dass nur einige beteiligten Stellen datenschutzrechtlich für die Videoüberwachung verantwortlich seien und die von der Veranstalterin umfangreich eingesetzten Kamerasysteme dazu genutzt werden sollten, sich anbahnende oder stattfindende Gefahren unter den anwesenden Fans zu erkennen. Dabei wurden beispielsweise Rohheitsdelikte, das Auftreten sicherheitsrelevanter Personengruppen oder auch sexuelle Übergriffe und das Auffinden verdächtiger Gegenstände angeführt. Die Veranstalterin trug vor, auf solche Situationen schnellstmöglich koordiniert geeignete Gegenmaßnahmen ergreifen zu wollen (bspw. Alarmierung der Polizei bei Gewaltausbrüchen / Ausschreitungen / Straftaten). Sie führte weiter an, dass im Falle einer Großschadenslage (die Veranstalter hatten hier wohl die Loveparade 2010 vor Augen) die Kamerabilder den Führungsstäben zur geregelten Besucherlenkung und zur Koordinierung von Rettungskräften dienen sollte.

Die private städtische Veranstalterin betonte an verschiedenen Stellen des Konzepts, dass der Einsatz der Videoüberwachungstechnik damit ein wichtiger Bestandteil des eigenen Sicherheitskonzepts, im Sinne der präventiven Maßnahmen, aber auch für die Lagebeurteilung im Eintrittsfall sei. Zudem sollten u. a. Maßnahmen zur Besucherlenkung unterstützt werden.

Nach einer ersten Sichtung der Unterlagen unmittelbar nach Eingang baten wir die Veranstalterin um ergänzende Erläuterungen, da offene Fragen blieben. Trotz nachgereichter Ergänzungen blieben die datenschutzrechtlichen Rollen der beteiligten Stellen und Unternehmen sowie die Rechtsgrundlagen, nach denen eine Verarbeitung personenbezogener Daten der Besuchenden, Markttreibenden und verschiedener Mitarbeitendengruppen (z. B. private Ordnungsdienste und Mitarbeitende an Ständen) verarbeitet werden sollten, unklar.

Neben dem Videoeinsatzkonzept der städtischen Gesellschaft war zwischenzeitlich auch das Polizeipräsidium Stuttgart an uns herangetreten und hatte uns über das polizeiliche Datenschutzkonzept Videobeobachtung UEFA EURO 2024 informiert.

Aufgrund der Komplexität des Vorhabens, der Vielzahl an Beteiligten und den offenen datenschutzrechtlichen Fragen mit Blick auf die organisatorische und technische Handhabung der verschiedenen Videoüberwachungskonzepte schlugen wir einen Austausch in unserer Behörde mit der Veranstalterin und den von ihr beauftragten Unternehmen vor.

Bei dem persönlichen Austausch Ende April mit einer Vertreterin der Stadt Stuttgart und verschiedenen Verantwortlichen des mit der Durchführung beauftragten Unternehmens der Stadt Stuttgart, einer externen Datenschutzbeauftragten und dem mit der technischen Umsetzung beauftragten Unternehmen wurde das uns bereits bekannte Videoeinsatzkonzept und die Gesamtsituation erörtert. Insbesondere wurden Fragen zu den Verantwortlichkeiten diskutiert und der Umstand thematisiert,

dass das Videoeinsatzkonzept der Veranstalterin neben der Videoüberwachung der Polizei installiert und in einem nicht unerheblichen Maß die gleichen Bereiche der Innenstadt videoüberwacht werden sollten. Betroffene würden also von zwei Systemen mit gleicher Ausrichtung aufgenommen. Des Weiteren wurde aufgezeigt, dass die Veranstalterin als Zwecke der Videoinstallation teilweise polizeiliche Aufgaben angab, sie zur entsprechenden Aufgabenwahrnehmung jedoch nicht berechtigt war. Zudem ging aus dem Konzept der Veranstalterin hervor, dass die Polizei keine Weisungsbefugnis gegenüber der Veranstalterin und dem mit der technischen Umsetzung beauftragten Unternehmen haben würde und das von der Veranstalterin beauftragte Unternehmen auch nicht als reine Auftragsverarbeiterin tätig werden sollte, sondern durch die eigene Einflussnahme auf die Ausrichtung der Kameras über Mittel und Zwecke der Verarbeitung mitentscheiden könne. Warum die Veranstalterin diese datenschutzrechtliche Konstellation wählte, blieb für uns bis zum Ende der Veranstaltung im Verborgenen.

Wir wiesen im Termin Ende April zunächst mündlich und später in weiteren schriftlichen Stellungnahmen bis Anfang Juni mehrfach darauf hin, dass aus unserer Sicht lediglich Art. 6 Abs. 1 Buchst. e), Abs. 3 DS-GVO in Verbindung mit § 18 LDSG für einen kleinen Teil der angegebenen Flächen, insbesondere den Schlossplatz, als Rechtsgrundlage für eine Videoüberwachung durch die Veranstalterin in Betracht käme. Auf dem Schlossplatz übte die Veranstalterin während der EURO 2024 über den abgegrenzten Bereich vor der Bühne und innerhalb der extra errichteten Buden und Absperrungen aufgrund der ordnungsrechtlichen Genehmigung der Stadt Stuttgart das Hausrecht im Sinne von Art. 6 Abs. 1 Buchst. e) DS-GVO in Verbindung mit § 18 LDSG aus. Die Außenbereichsüberwachung auf dem Schlossplatz diente damit der Schutzfunktion des § 18 Abs. 1 Nr. 2 LDSG. Der hierbei wesentlichen präventiven Zielrichtung der Norm wurde die Veranstalterin insbesondere gerecht, weil eine kontinuierliche Beobachtung der übertragenen Bilder in Echtzeit im HCOC sichergestellt war.

Andere öffentlich zugängliche Bereiche wie z. B. die Königstraße oder der Karlsplatz hingegen fallen nicht in den Anwendungsbereich von § 18 Abs. 1 LDSG, so sind sie weder öffentliche Einrichtung im Sinne von Nr. 1 noch handelt es sich bei der Videoüberwachung von Straßen und Plätzen um sonstige bauliche Anlagen oder in unmittelbarer Nähe befindliche Sachen im Sinne von § 18 Abs. 1 Nr. 2 LDSG. Eine Rechtsgrundlage für die beabsichtigte Videoüberwachung durch die Veranstalterin war daher nicht gegeben. Mehrfach wurde hervorgehoben, dass die gesetzlichen Voraussetzungen für die Installation bei jeder einzelnen beabsichtigten Kamera geprüft werden müssen.

Schließlich wurde bei einem Vor-Ort-Termin im HCOC am 13. Juni 2024 verbindlich festgelegt, dass lediglich die temporäre Videoüberwachung des Schlossplatzes datenschutzrechtlich zulässig war und für die weiteren eingesetzten Videokameras von der Veranstalterin und ihren beauftragten Unternehmen physische Verpixelung angebracht werden mussten. Bis zur Auftaktveranstaltung am 14. Juni 2024 wurden entsprechende physische Maßnahmen zur Verschlechterung der Bildauflösung bei einer Vielzahl von Kameras durch die Veranstalterin angebracht und alle Kameras datenschutzkonform ausgerichtet. Auch bei einer weiteren Kontrolle im Veranstaltungszeitraum überzeugten wir uns vor Ort davon, dass alle rechtlichen Vorgaben eingehalten wurden. Lediglich nach dem Vorfall auf dem Schlossplatz, bei welchem die Polizei die Kameras zur Unterstützung nutzte, waren erneut datenschutzrelevante Änderungen der Einstellung erforderlich. Zusammen mit den Beteiligten wurde erneut eine datenschutzkonforme Einstellung der Kameras auf dem Schlossplatz getroffen und die Verantwortlichen über die Rechtslage aufgeklärt.

Insgesamt blieb für uns bis zum Ende der EURO 2024 unklar, warum die Veranstalterin und die Polizei nicht ein Gesamtkonzept für den Einsatz einer Videoüberwachung im Stadtgebiet erstellten. Während die Polizei ihre Videoüberwachung der Innenstadt in dieser Zeit auf § 44 Abs. 1 Nr. 2 PolG stützen konnte, war ein entsprechender paralleler Einsatz von Videotechnik durch die Veranstalterin bei einer Vielzahl von Fällen auf Grundlage von § 18 Abs. 1 Nr. 2 LDSG nicht möglich.

Einfach mal Aufnahmen machen und der Polizei schicken? In einem Fall, den sich der LfDI angesehen hat, war das keine gute Idee.

Wächter für die Polizei

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

Warum den Wächter-Modus nicht als Ermittlungshelfer nutzen? Diese Idee kam einer Polizeidienststelle, die eine Serie von Autoaufbrüchen bearbeitete und mit Hilfe der Halter von Tesla-Fahrzeugen aus einem bestimmten Stadtgebiet neue Ermittlungsansätze gewinnen wollte.

Die Polizeidienststelle machte Tesla-Besitzer_innen im Stadtgebiet mittels Halterdatenabfrage ausfindig und schrieb sie an. In dem Schreiben wurde den Betroffenen empfohlen, den Wächter-Modus des Tesla-Fahrzeuges über Nacht zu aktivieren, wenn dieses in einer Tiefgarage abgestellt wurde und mögliche verdächtige Aufnahmen an die Polizei zu übersenden. Von der Videoüberwachung der Fahrzeuge sowie ihrer Umgebung erhoffte sich die Polizei Erkenntnisse für ihre Ermittlungen. So waren zuvor in mehreren Fällen Fahrzeugteile wie Sensoren oder Spiegel von in privaten Tiefgaragen abgestellten Autos entwendet worden. Jenseits von einer Annäherung waren vom Hersteller Tesla jedoch keine Fahrzeuge betroffen.

Die Vorgehensweise der Polizeidienststelle sorgte in einem Internetforum der Tesla-Community für heftige Diskussionen. Ein Teilnehmer nahm dies zum Anlass, die Frage der Rechtmäßigkeit des polizeilichen Handelns an uns heranzutragen.

Nach eingehender Prüfung waren sowohl die Abfrage der Fahrzeughalterdaten, als auch das Schreiben mit der Aufforderung, den Wächter-Modus zu aktivieren und verdächtiges Videomaterial an die Polizei weiterzugeben, datenschutzrechtlich zu beanstanden.

Zur Prüfung im Einzelnen

Die angeführte Rechtsgrundlage des § 35 Abs. 1 Nr. 2 und Nr. 4 StVG zum Abruf der Daten beim Kraftfahrtbundesamt war nicht ausreichend. Denn nach dem Doppeltürmodell des Bundesverfassungsgerichts (BVerfG, Beschl. v. 24.01.2012, AZ: 1 BvR 1299 / 05, Rn. 123.) bedarf es sowohl für die Übermittlung von personenbezogenen Daten durch zum Beispiel das Kraftfahrbundesamt, als auch für den Abruf der Daten durch die Polizeibehörden jeweils eigener Rechtsgrundlagen.

Als Befugnisnorm der Polizei kommt für Halterdatenabfragen zum Zweck der Gefahrenabwehr § 36 Abs. 2 Nr. 1 d) StVG in Verbindung mit § 43 Abs. 3 Polizeigesetz Baden-Württemberg (PolG BW) in Betracht. Für Zwecke der Strafverfolgung durch die Polizei ist dies in § 36 Abs. 2 Nr. 1 c) in Verbindung mit § 163 Abs. 1 Strafprozessordnung geregelt.

Für einen Abruf im automatisierten Verfahren gemäß §§ 36 Abs. 2 Nr. 1 d) StVG, 43 Abs. 3 Polizeigesetz Baden-Württemberg (PolG BW) zum Zwecke der Gefahrenabwehr fehlte es vorliegend jedoch an einer hinreichend konkreten Gefahr für die betroffenen Tesla-Halter.

Beim zu prüfenden Sachverhalt war bei den über 200 Straftaten nur in einem Fall ein Tesla Fahrzeug betroffen. Die Gefahrenlage für die angeschriebenen Tesla-Fahrzeughalter erschien daher eher abstrakt, da zum Zeitpunkt der Abfrage zwar ein gewisses Gefahrenpotential bestand, aber ein sofortiges Einschreiten noch nicht erforderlich war. §§ 43 Abs. 3; 70 Nr. 4 PolG BW erlaubt jedoch die Datenerhebung nur bei Personen, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass gerade sie Opfer einer Straftat werden. Ausreichend ist daher nicht, dass tatsächliche Anhaltspunkte dafür vorliegen, dass allgemein Personen, die Halter von Tesla-Fahrzeugen sind, Opfer einer Straftat werden könnten, weil es sich bei Tesla-Fahrzeugen um Fahrzeuge der Oberklasse und damit potentielle Tatobjekte handelt. Erforderlich für eine Datenerhebung ist vielmehr, dass tatsächliche Anhaltspunkte dafür vorliegen, dass konkret diese Tesla-Halter, deren Daten abgefragt werden sollen, Opfer einer Straftat werden könnten. An entsprechenden Anhaltspunkten für eine konkrete Gefahr fehlte es hier indes. Auch ist die Maßnahme der Halterabfrage weder vollständig geeignet noch erforderlich, die richtigen Personen anzuschreiben. Denn der Aufbewahrungsort für die Fahrzeuge stimmte nicht zwingend mit der Halteranschrift überein. Für Halter, die zwar in der betroffenen Stadt ihren (Wohn-)Sitz hatten, aber ihr Fahrzeug dort nicht aufbewahrten, war die Datenerhebung nicht erforderlich. Umgekehrt war die Datenverarbeitung nicht geeignet, Halter zu erreichen, die ihr Fahrzeug in der betroffenen Stadt aufbewahrten, aber ihre (Wohn-)Sitze dort nicht hatten.

Ein Abruf zum Zwecke der Strafverfolgung gem. § 36 Abs. 2 Nr. 1 c) StVG i.V.m. § 163 Abs. 1 StPO schied in der konkreten Fallkonstellation ebenfalls aus, da es an konkreten Straftaten zu Lasten der Tesla-Halter fehlte.

Auch das Hinweisschreiben war aus unserer Sicht nicht mit den Vorgaben des polizeilichen Datenschutzrechts vereinbar. Bei der Erhebung personenbezogenen Daten Dritter durch den Tesla-Wächter-Modus handelte es sich um einen mittelbaren Grundrechtseingriff, da das Hinweisschreiben kausale Ursache der Aktivierung des Wächter-Modus war. Somit ging die Datenerhebung letztlich auf staatliches Handeln zurück bzw. war diesem zurechenbar. Diese Einschätzung wird noch dadurch verstärkt, dass das Hinweisschreiben auch die Anmerkung enthielt, die Fahrzeughalter sollten sich nicht scheuen, die Polizei zu kontaktieren, wenn ihr Fahrzeug verdächtige Personen aufzeichnet. Hintergrund dieser Formulierung war offensichtlich der Wunsch der Verfasser des Hinweisschreibens, letztlich die Bilddaten verdächtiger Personen übermittelt zu bekommen. Der potentielle Grundrechtseingriff war somit aus unserer Sicht nicht nur in dem von einem aktivierten Wächter-Modus ausgehenden präventiven Abschreckungseffekt zu sehen, sondern auch in der repressiv wirkenden Möglichkeit der Erhebung von Beweismaterial zum Zwecke strafprozessualer Ermittlungen.

Für einen solchen Eingriff in die informationelle Selbstbestimmung Dritter fehlte es jedoch an einer Rechtsgrundlage. Insbesondere war der von der Polizei vorgetragene § 29 Abs. 2 PolG BW i.V.m. Art. 6 Abs. 1 Buchst. f) DS-GVO keine taugliche Rechtsgrundlage für eine durch das Hinweisschreiben „veranlasste“ Datenerhebung. Denn zum einen zielt § 29 Abs. 2 PolG BW auf die Verhinderung von Straftaten und deren nachteilige Folgen für die Betroffenen ab (Enders in: Möstl / Trurnit, BeckOk PolR BW, 30. Ed., § 29 PolG BW, Rn. 19 f.). Die Erhebung von Beweismaterial zu repressiven Zwecken ist somit vom präventiven Charakter der Norm nicht umfasst. Zum anderen begründete das vorliegende Hinweisschreiben eine unzulässige Vermischung staatlicher Strafverfolgungstätigkeit mit den Möglichkeiten privater Datenverarbeitung. Denn die Datenerhebung mag zwar von der freiwilligen Umsetzung des Hinweises auf die Möglichkeiten des Wächter-Modus durch den jeweiligen Fahrzeughalter abhängen. Den eigentlichen Datenerhebungsvorgang führte somit ein privater Akteur aus. Es handelte sich dadurch aber faktisch um eine Ausführung staatlicher Ermittlungsarbeit

durch private Akteure. Eine solche Einbindung von Tesla-Haltern in polizeiliche Maßnahmen mittels eines Hinweisschreibens ist höchst problematisch, da der Staat sich auf diese Weise bei seiner Aufgabenerfüllung privater Akteure bedient oder diese zumindest dazu „ermutigt".

Dies führt im Ergebnis dazu, dass die staatliche Stelle ihre Befugnisse faktisch erweitert (s. dazu auch Bäcker in: Lisken / Denninger, HdB d. PolR, 7. Aufl., 2021, Rn. 282). Bundes- und Landesgesetzgeber haben für die Gefahrenabwehr und Strafverfolgung im PolG BW und der StPO jedoch eigene Rechtsgrundlagen mit entsprechenden Tatbestandsvoraussetzungen für die Erhebung von Bilddaten geschaffen. Diese würden umgangen, wenn die Einbindung Privater die Anwendbarkeit von Art. 6 Abs. 1 Buchst. f) DS-GVO ermöglichen würde.

Diese Wertung vollzieht auch das unionale Datenschutzrecht nach, indem Art. 6 Abs. 1 S. 2 DS-GVO klarstellt, dass die Rechtsgrundlage des Art. 6 Abs. 1 Buchst. f) DS-GVO nicht für Behörden in Erfüllung ihrer Aufgaben anwendbar ist. Selbst wenn man also die Erhebung von Bilddaten durch private Akteure zum Zwecke der Gefahrenabwehr und Strafverfolgung als verfassungsrechtlich zulässig ansehen würde, so würde der „Umweg" über einen privatrechtlichen Akteur, der den Datenerhebungsvorgang letztlich ausführt, jedenfalls zu einer datenschutzrechtlich unzulässigen Umgehung der Wertung des Art. 6 Abs. 1 S. 2 DS-GVO führen. Zwar hat der BGH betont, dass die von Privaten erzeugten Bildaufnahmen selbst dann keinem Beweisverwertungsverbot unterliegen, wenn diese unter Verstoß durch das Datenschutzrecht erstellt wurden (BGH, Beschl. v. 18. August 2021, AZ 5 StR 217 / 21, Rn. 5.). Aus der zulässigen strafprozessualen Verwertung der Daten folgt jedoch nicht, dass auch eine (mittelbare) Veranlassung der Erhebung der Daten zulässig ist.

Die Annahme einer Rechtsgrundlage, die sich aus der staatlichen Befugnis zur Gefährdetenansprache des § 29 Abs. 2 PolG BW in Verbindung mit dem für den Staat in Erfüllung seiner Aufgaben gesperrten Art. 6 Abs. 1 Buchst. f) DS-GVO zusammensetzt, überzeugte daher im Ergebnis nicht.

Ein Informationsschreiben darf unserer Auffassung nach nicht mit einem Hinweis versehen sein, die Bürgerinnen und Bürger sollten sich „nicht scheuen", entsprechend erzeugte Aufnahmen an die Polizei zu übermitteln. Denn dann handelt es sich nicht mehr nur um einen zulässigen staatlichen Hinweis auf die Möglichkeiten des Selbstschutzes, sondern faktisch um eine Veranlassung einer staatlichen Überwachungsmaßnahme unter Einbindung privater Videoüberwachungstechnik. Eine solche Veranlassung geht dann auch über eine bloß mittelbare „Grundrechtsbeeinträchtigung" (siehe dazu näher Voßkuhle / Kaiser, JuS 2018, 343 (344)) durch staatliches Informationshandeln hinaus, für die das BVerfG eine eigene Rechtsgrundlage verlangt, wenn sich die Einwirkung auf die Grundrechte der Betroffenen letztlich als Ersatz bzw. Äquivalent zu staatlichem Handeln erweist (BVerfGE 105, 279 (303). Diese Schwelle ist jedenfalls dann überschritten, wenn mittels eines Hinweisschreibens private Videoaufnahmen veranlasst und zugleich gezielt als Beweismittel hergestellt werden sollen.). Für die Frage, ob ein Grundrechtseingriff oder „nur" eine mittelbare Beeinträchtigung vorliegt, kommt es unseres Erachtens nach letztlich darauf an, ob die staatliche Informationsmaßnahme primär auf eine Stärkung der Grundrechtsausübung der informierten Bürgerinnen und Bürger oder auf einen Eingriff in ein Grundrecht der letztlich am Ende der „Kette" betroffenen potentiellen Personen abzielt (so auch Lenski, ZJS 2008, Heft 1, S. 13 (17)). Ersteres wäre bei einer allgemeinen Information über Schutzmöglichkeiten für die informierten Personen der Fall. Hier würde die Information ihre Möglichkeiten stärken, eigene Maßnahmen zum Schutz des eigenen KfZ (und damit des Eigentums) ergreifen zu können. Dagegen würde es sich bei einer Information, die letztlich auf einen staatlich erwünschten Eingriff in die informationelle Selbstbestimmung potentieller Straftäter abzielt, primär um einen gewollten Eingriff in deren Grundrecht zum Zweck der Strafverfolgung handeln, bei dem die Stärkung der Grundrechtsausübung der informierten Personen nur Mittel zum Zweck ist. Unzulässig ist es daher unserer Auffassung nach auch, wenn Sicherheitsbehörden zwar auf eine entsprechende „Anregung" zur Übersendung von Beweisvideos verzichten, das Hinweisschreiben jedoch be-

reits mit der Intention versenden, im Nachgang bei den Empfängern systematisch Videoaufnahmen zu Beweiszwecken abzufragen.

Nach Prüfung des vorgelegten Sachverhalts kamen wir zu dem Schluss, dass sowohl die Abfrage der Fahrzeughalterdaten, als auch das Schreiben mit der Aufforderung, den Wächter-Modus zu aktivieren und verdächtiges Videomaterial an die Polizei weiterzugeben, datenschutzrechtlich unzulässig waren. Die Diebstahlserie konnte übrigens zwischenzeitlich aufgeklärt werden und zwar auch ohne die Einsendung von Videoüberwachungsmaterial durch Tesla-Besitzer_innen.

Teslas Wächter-Modus

Wird der Wächter-Modus oder Sentry Mode bei abgestellten Tesla-Fahrzeugen aktiviert, bleiben Kameras und Sensoren aktiv und überwachen Fahrzeug und Umgebung (mittlerweile optional). Wird eine „mögliche Bedrohung" (Tesla) erkannt, speichern die Kameras ihre Aufnahmen auf einem USB-Stick und benachrichtigen die Besitzer_in per App. Mit dieser kann auch direkt auf die Kameras zugegriffen werden.

Letztlich handelt es sich dabei um eine – häufig rechtswidrige – Videoüberwachung. Tesla sieht die Fahrzeugbesitzer_innen in der Verantwortung „alle vor Ort geltenden Vorschriften und Eigentumsvorbehalte im Hinblick auf die Verwendung von Kameras zu prüfen und einzuhalten." Auch die betroffene Polizeidienststelle hat in ihrem Schreiben darauf hingewiesen, dass der Einsatz von Videoüberwachung in der Öffentlichkeit nicht erlaubt ist. Dieser rechtliche Hinweis sei jedoch unvollständig, betonte die Polizei später. Auch jenseits der Öffentlichkeit kann der Einsatz des Wächter-Modus illegal sein.

tesla.com/ownersmanual/models/de_us/GUID-56703182-8191-4DAE-AF07-2FDC0EB64663.html

☛ Weitere Informationen

36. Tätigkeitsbericht Datenschutz des LfDI BW, „Mein Auto sieht Dich!" – Tesla & Co: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf S. 108 ff.

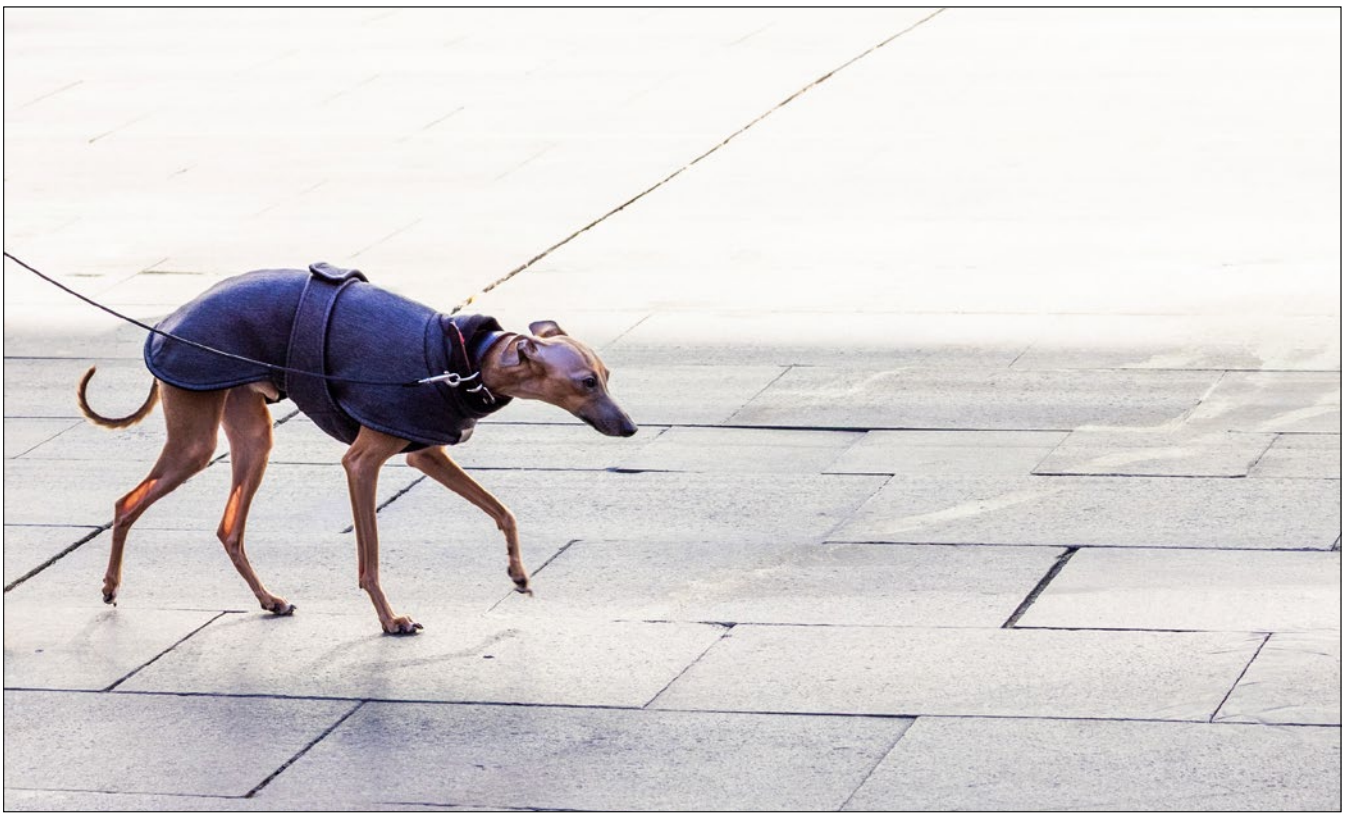
39. Tätigkeitsbericht Datenschutz des LfDI BW, Wächtermodus geht auch anders: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf

Ordnung muss sein – von Falschparkern und Hunde-DNA

✎ Art. 57 Abs. 1 Buchst. f) DS-GVO

Im Zusammenhang mit der Anzeige und Verfolgung von Ordnungswidrigkeitenstellen stellen sich den betroffenen Bürger_innen und den verantwortlichen Stellen immer wieder auch datenschutzrechtliche Fragen. Dabei können Ordnungswidrigkeiten ganz unterschiedliche Lebenssachverhalte und Regelungsmaterien betreffen, wie unsere folgenden beiden Beispiele zeigen.

In diesem Jahr wurde an uns vermehrt die Frage herangetragen, ob im Zusammenhang mit Privatanzeigen von Ordnungswidrigkeiten das Fertigen von Fotos zumeist von falsch parkenden Fahrzeugen und deren Weiterleitung an das Ordnungsamt einen Verstoß gegen datenschutzrechtliche Vorschriften darstelle, da zumindest das Kennzeichen ein personenbezogenes Datum sei. Diesen Personen haben wir mitgeteilt, dass wir darin, dass Fotos falsch parkender Fahrzeuge durch Private an Behörden, hier insbesondere an das Ordnungsamt, geschickt werden, grundsätzlich keinen Verstoß gegen datenschutzrechtliche Vorschriften se-



© kwasibanane

Kreative Idee, aber nicht machbar: Eine Kommune wollte eine DNA-Datenbank für Hunde einrichten und hier lag das Problem: mit der Verknüpfung zu den jeweiligen Halter_innen.

hen. Denn für hinweisgebende Personen kann ein dahingehendes berechtigtes Interesse bestehen. Die zuständige Behörde entscheidet sodann nach eigenem Ermessen, ob sie der Meldung nachgeht oder nicht. Allerdings müssen dabei durch die hinweisgebenden Personen die datenschutzrechtlichen Grundsätze eingehalten werden. Unter anderem ist der Grundsatz der Datenminimierung zu beachten, insbesondere, dass die Verarbeitung personenbezogener Daten unbeteiligter Dritter unterbleibt. Auch bei der Übermittlung an die zuständige Behörde ist darauf zu achten, dass die Art und Weise der Übermittlung den datenschutzrechtlichen Anforderungen entspricht; darauf haben sowohl die hinweisgebenden Personen, als auch die ggf. einen Übermittlungsweg bereitstellende Stelle als jeweils datenschutzrechtlich Verantwortliche zu achten.

Anderes gilt für die Veröffentlichung von Fotos von falschparkenden Fahrzeugen mit erkennbarem Kennzeichen im Internet. Hierfür gibt es keine Rechtsgrundlage, eine Veröffentlichung ist unzulässig.

Mit einer eher ausgefallenen Idee wollte eine Kommune in Baden-Württemberg der nichtrechtmäßigen Entsorgung von Hunde-Kot entgegenwirken. So sollte mittels DNA-Analyse der unsachgemäß entsorgten Hinterlassenschaft eines Hundes herausgefunden werden, welchem Hund diese zuzuordnen ist, damit die Halterin oder der Halter des Hundes entsprechend sanktioniert werden kann. Hierfür sollte eine DNA-Datenbank aller Hunde der Kommune erstellt werden, dies natürlich in Verbindung mit den Daten der Halterin oder des Halters, sodass sich die Frage stellte, ob es hierfür eine datenschutzrechtliche Rechtsgrundlage gibt. Bereits der behördliche Datenschutzbeauftragte stand dem Vorhaben skeptisch gegenüber. Und auch wir konnten nach Überprüfung des Sachverhaltes keine datenschutzrechtliche Rechtsgrundlage finden, welche die Errichtung einer solchen Datenbank erlaubt. Möglicherweise

waren die Mitarbeitenden des Ordnungsamtes dem Datenschutz für diese Einschätzung dankbar.

Diese Beispiele zeigen, dass auch im Zusammenhang mit Ordnungswidrigkeiten datenschutzrechtliche Belange immer mitbedacht werden müssen. Der Datenschutz steht weder der Anzeige noch der Verfolgung von Ordnungswidrigkeiten generell entgegen. Auch hier gilt: eine Rechtsgrundlage muss vorhanden sein und die datenschutzrechtlichen Grundsätze beachtet werden.

Vollautomatische Standseilbahn mit Videosensoren

✎ Art. 57 Abs. 1 Buchst. c) DS-GVO

In einem Karlsruher Planfeststellungsverfahren zum Umbau einer Standseilbahn waren verschiedene Einwendungen eingegangen. Diese richteten sich insbesondere gegen die Videotechnik, die für den vollautomatischen Betrieb der Standseilbahn an den Fahrzeugen installiert werden soll. Die Bahn soll im Bereich mehrerer Grundstücke verkehren, weshalb die Anwohner_innen befürchteten, durch den Videobetrieb in datenschutzrechtlich unzulässiger Weise betroffen zu sein. Wir wurden daraufhin zur Frage der Zulässigkeit der Videotechnik beteiligt.

Falls Sie das nicht ganz alltägliche Verkehrsmittel „Standseilbahn" noch nicht kennen, möchten wir es Ihnen kurz vorstellen: Standseilbahnen werden, wie der Name schon sagt, durch Seile bewegt. Im Gegensatz zu Luftseilbahnen fahren sie auf Schienen oder anderen Führungen. Die Wagen einer Standseilbahn können große Höhenunterschiede überwinden.

Mit Hilfe von Videosensoren an den Fahrzeugen der Standseilbahn, die insbesondere an der Fahrzeugfront im Außenbereich angebracht werden, soll ein vollautomatischer Betrieb der Bahn gewährleistet werden. Das bedeutet, dass kein Fahrpersonal mehr in den Fahrzeugen selbst anwesend sein muss, um diese zu steuern. Der Zugriff auf die Kameras soll im Regelbetrieb durch die Fernleitstelle des Verkehrsunternehmens erfolgen. Sie sind als Videolösung zur Live-Betrachtung (sog. Monitoring) vorgesehen. Eine dauerhafte Live-Betrachtung während des Fahrbetriebs erfolgt dabei nicht. Die Streckenüberwachung soll nur anlassbezogen zur Betriebsaufnahme morgens durch die Leitstelle (durch Leerfahrten, d. h. ohne Fahrgäste) sowie zur Überprüfung der Befahrbarkeit der Trasse bei besonderen Ereignissen (bei einem Stillsetzen der Bahn auf der Strecke, bei außergewöhnlichen Witterungsverhältnissen, bei dem Ansprechen einer Fluchttürüberwachung) dienen. Der Fahrbereich der Standseilbahn wird auf der gesamten Strecke entsprechend den Vorgaben einer Sicherheitsvorschrift (DIN-Norm) für „Standseilbahnen mit automatischem Betrieb" eingezäunt. Die Zaunhöhe beträgt demnach weitestgehend 1,80 m und wird nur im oberen, nicht innerstädtischen Bereich der Trasse auf 1,20 m Höhe reduziert. Eine Verpixelung des Kamerabildes in Bereichen außerhalb des Zaunes soll das Sichtfeld der Kameras auf die Trasse beschränken. Außerdem ist die Strecke nur für das Instandhaltungs- und Werkstattpersonal zugänglich. Weitere Sensoren zur Streckenüberwachung sind nicht vorgesehen.

Der datenschutzrechtlich Verantwortliche für den Kamerabetrieb, das Verkehrsunternehmen, ist eine juristische Person des Privatrechts. Sie befindet sich zwar vollständig im Besitz der öffentlichen Hand. Da das Unternehmen jedoch im Wettbewerb mit anderen Verkehrsträgern steht, gilt eine landesrechtliche Verweisnorm, § 2 Abs. 6 Landesdatenschutzgesetz BW. Nach dieser sind in einem solchen Fall die für nicht-öffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden. Die Zulässigkeit der Verarbeitung personenbezogener Daten mittels der Fahrzeugkameratechnik beurteilt sich daher im Wesentlichen nach Art. 6 Abs. 1 Buchst. f) DS-GVO. Nach dieser Norm kann eine Verarbeitung rechtmäßig sein, soweit diese zur Wahrung berechtigter Interessen des Verantwortlichen oder Dritter erforderlich ist und nicht die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen, deren Daten verarbeitet werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen überwiegen.

Das Interesse an einem vollautomatischen Betrieb der Standseilbahn ist ein berechtigtes Interesse. Der automatische Betrieb von Standseilbahnen ist

in einer Sicherheitsvorschrift (DIN-Norm) sogar als Betriebsart ausdrücklich anerkannt.

Das Videosystem an den Fahrzeugen ist auch für den Betrieb der Standseilbahn erforderlich. Aus der einschlägigen DIN-Norm, die den automatischen Betrieb vorsieht, ergeben sich zwar keine direkten Aussagen zur Ausgestaltung der Systeme, die der Automatisierung des Betriebes dienen. Für Zwecke wie das Erkennen denkbarer Gefahrensituationen, z. B. von im Gleis liegenden Gegenständen oder besonderen Witterungsverhältnissen, die Teile der Strecke beeinträchtigen, erscheint der Einsatz von Videotechnik jedoch geeignet. Zur Erkennung von sicherheitsgefährdenden Vorgängen oder schädigenden Handlungen ist die Erforderlichkeit von Videotechnik grundsätzlich anerkannt. Anstelle des Einsatzes sind keine Mittel ersichtlich, die den automatischen Betrieb in gleicher Weise gewährleisten und weniger intensiv in die Rechte und Interessen der Betroffenen (z. B. der Anwohner und sonstigen Verkehrsteilnehmer) eingreifen. Es sind keine Gründe ersichtlich, die der Erforderlichkeit des Einsatzes von Videosystemen zur Gewährleistung des vollautomatisierten Betriebs der Turmbergbahn generell entgegenstehen.

Bei der notwendigen Abwägung der berechtigten Interessen des datenschutzrechtlich verantwortlichen Verkehrsunternehmens am vollautomatischen Betrieb der Standseilbahn mit den Rechten und Interessen der Betroffenen, u. a. an deren unbeobachteter Teilnahme am öffentlichen Leben und an der Achtung des Privat- und Familienlebens der Anwohner_innen, überwiegen die Interessen der Betroffenen im Ergebnis nicht. Dies liegt zum einen daran, dass sich die Streckenüberwachung zeitlich auf die Betriebsaufnahme und besondere betriebsrelevante Ereignisse beschränken soll, die eine Sichtkontrolle erforderlich machen. Damit werden der Kamerabetrieb und die hiermit verbundene mögliche Verarbeitung personenbezogener Daten zeitlich minimiert. Zum anderen wird der von den Kameras einsehbare Bereich durch eine Verpixelung gleichzeitig räumlich begrenzt. Es werden nur die durch die Zäune abgesperrten Gleisbereiche und deren direktes Umfeld beobachtet. Insofern werden Anwohnerbereiche, die außerhalb des Zaunes liegen, durch die Verpixelung vor der Beobachtung geschützt. Die nicht verpixelten Beobachtungsbereiche sind ohnehin nicht für den Aufenthalt von Unbefugten vorgesehen, weshalb kein überwiegendes Interesse von Unbefugten, die sich auf den Gleisen aufhalten, erkennbar wäre, welches gegenüber dem Interesse des Verantwortlichen überwiegen könnte. Darüber hinaus haben wir den Verantwortlichen darauf hingewiesen, dass die Sicherheit des Zugriffs auf die Kamerabilder (insbesondere hinsichtlich Anlass, zeitlichem Umfang, Berechtigung der zugreifenden Personen und Zweck des Zugriffs) durch geeignete technische und organisatorische Maßnahmen zu gewährleisten ist. Darüber hinaus sind die Kameras so auszurichten und einzurichten (auch hinsichtlich der technischen Ausstattung wie Auflösung, Blenden etc.), dass eine Verarbeitung personenbezogener Daten, soweit sie nicht zur Zweckerreichung erforderlich ist, vermieden wird. Insgesamt können die Rechte und Interessen der Betroffenen somit grundsätzlich gewahrt werden.

Die Verarbeitungen personenbezogener Daten im Rahmen einer Videobeobachtung an den Fahrzeugen der Standseilbahn für einen vollautomatischen Betrieb sind daher nach Art. 6 Abs. 1 Buchst. f) DS-GVO datenschutzrechtlich rechtfertigbar.

Im Ergebnis konnten wir „grünes Licht“ geben, das geplante Vorhaben eines vollautomatischen Betriebs erscheint nach dem letzten Planungsstand zumindest aus datenschutzrechtlicher Perspektive grundsätzlich realisierbar.

KI-Anwendungen in Schwimmbädern

✎ Art. 57 Abs. 1 Buchst. a) DS-GVO

Die Künstliche Intelligenz (KI) nimmt Einzug in immer mehr unserer Lebensbereiche. Mittlerweile findet sie sich auch in Schwimmbädern wieder. Eingesetzt wird sie dort zur Ertrinkendenerkennung und zur Erkennung kritischer Situationen. Ziel ist es, Bademeister_innen zeitig zu warnen und ihnen die Möglichkeit zu geben zu handeln, noch bevor es zu einem Ertrinkungsfall kommt. Dies soll Bade-

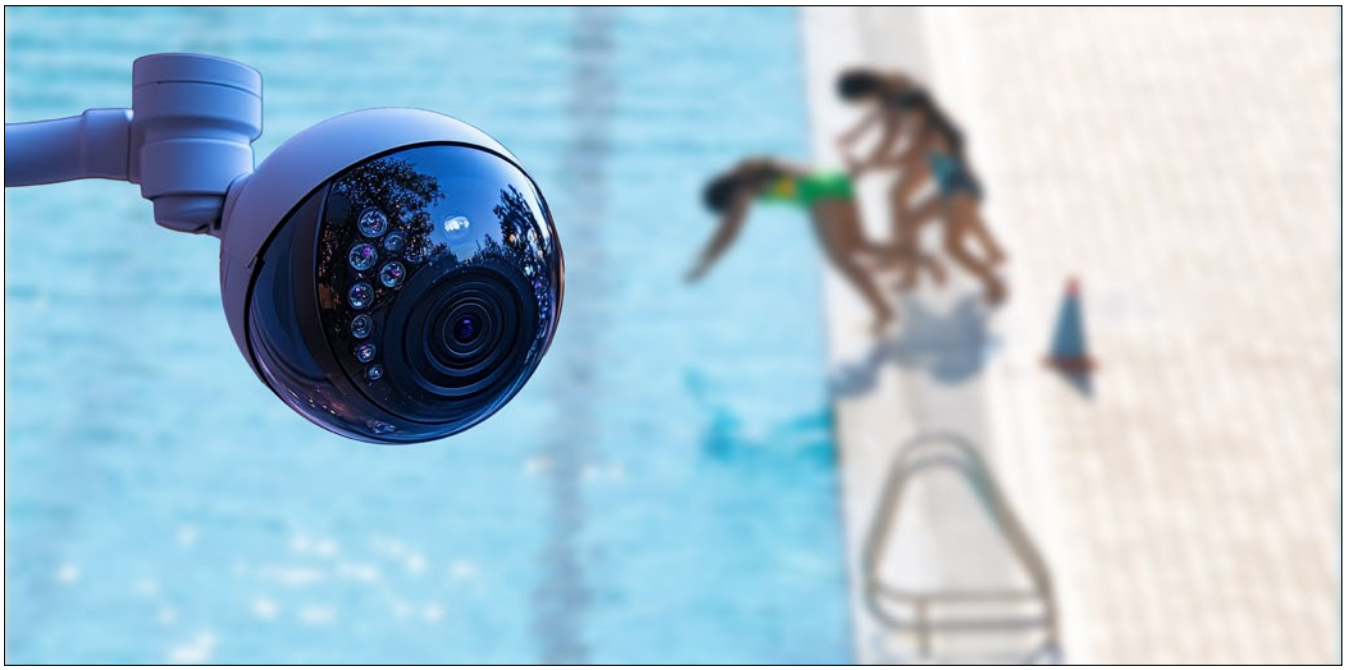
meister_innen bei ihrer Arbeit unterstützen und die Schwimmsicherheit in den Bädern erhöhen. Doch was gilt es datenschutzrechtlich bei der Einführung eines solchen Systems zu beachten? Mit dieser Frage haben wir uns dieses Jahr befasst und zwei Schwimmbäder, die eine solche Technik einsetzen, kontrolliert.

Beim Einsatz von KI-Systemen in Schwimmbädern werden Kameras über den Becken angebracht, die den Schwimmbetrieb erfassen. Die Aufnahmen werde an einen Server übermittelt, auf dem eine Echtzeitverarbeitung der Bilder durch die KI erfolgt. Verkürzt gesagt, soll die KI anhand der Bildaufnahmen Bewegungsmuster erkennen und eine Sicherheitswarnung ausgeben, wenn sie ungewöhnliche Bewegungsmuster feststellt. Diese Sicherheitswarnung u. a. mit der Angabe des betroffenen Beckens und des Standorts, an dem das ungewöhnliche Bewegungsmuster festgestellt wurde, wird auf Smartwatches übermittelt, die die Bademeister_innen tragen. Diese können daraufhin das betroffene Becken aufsuchen und kontrollieren, ob ein Gefahrenfall vorliegt und entsprechend reagieren.

Datenschutzrechtlich stellt sich die Frage, ob durch die Aufnahme der Videobilder und die Weiterverarbeitung durch die KI eine Datenverarbeitung i. S. d. der DS-GVO vorliegt. Dies wäre beispielsweise nicht der Fall, wenn die Aufnahmen so unscharf oder verpixelt sind, dass es sich bei den Bildaufnahmen nicht um personenbezogenen Daten i. S. d. Art. 4 Nummer 1 DS-GVO handelt.

Damit die KI die Möglichkeit hat, Bewegungsmuster zu erkennen und damit auch ungewöhnliche Bewegungsmuster zu detektieren, darf das Bild jedoch nicht zu unscharf sein. Es ist daher grundsätzlich davon auszugehen, dass es sich bei den Bildaufnahmen um personenbezogene Daten handelt.

Es gilt daher, wie bei jeder Verarbeitung personenbezogener Daten, das Erfordernis einer entsprechenden Rechtsgrundlage. Für die Bäder in öffentlicher Hand, die beispielsweise als Eigenbetriebe geführt werden, gilt das LDSG. Hier regelt § 18 LDSG (i.V.m. Art. 6 Abs. 1 Buchst. e), Abs. 3 DS-GVO) die Videoüberwachung öffentlich zugänglicher Räume. Nicht durch § 18 LDSG erfasst ist jedoch die Weiterverarbeitung und Bewertung der Bildaufnahmen mittels einer KI. Eine Rechtsgrundlage für die Verarbeitung von personenbezogenen Bilddaten durch eine KI wurde durch den Landesgesetzgeber bislang nicht geschaffen.



KI-Anwendungen im Schwimmbad? Erst prüfen, ob es dafür eine Rechtsgrundlage gibt.

Anders sieht es aus bei privatwirtschaftlich betriebenen Bädern. Dies gilt nach § 2 Abs. 6 Satz 1 LDSG auch, wenn öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen. Rechtgrundlage ist für diese Bäder im Regelfall Art. 6 Abs. 1 Buchst. f) DS-GVO. Die Verarbeitung der personenbezogenen Daten ist danach rechtmäßig, wenn diese 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.

Im Rahmen der Interessenabwägung wird von Seiten der Schwimmbäder eingebracht, mithilfe der KI eine möglichst große Sicherheit für die Besuchenden herzustellen, um im Notfall schnell eingreifen zu können. Im Idealfall sollte ein Notfall gar verhindert werden. Auf Seiten der Besuchenden steht dem entgegen, sich im Schwimmbecken bewegen zu können, ohne von Kameras aufgezeichnet zu werden. Dies auch vor dem Hintergrund, dass man sich typischerweise lediglich leicht bekleidet in Schwimmbecken aufhält. Hinzu kommt, dass für Besuchende gerade nicht klar ist, was mit ihren Bildern passiert, wenn diese durch die KI verarbeitet werden.

Die Frage, ob eine solche KI-Videoüberwachung zulässig ist, muss im Einzelfall für jedes Bad und gegebenenfalls für jedes Becken gesondert beurteilt werden. Hierbei ist beispielsweise das Gefahrenpotential eines Beckens zu berücksichtigen.

Soll ein solches KI-System implementiert werden, müssen sich die Badbetreiber_innen im Vorfeld Gedanken dazu machen, auf welche Rechtsgrundlage eine KI basierte Videoüberwachung gestützt werden kann und wie man hierbei den Eingriff in das Persönlichkeitsrecht der Besuchenden möglichst gering hält, ohne den eigentlichen Zweck – die Ertrinkendenerkennung – zu gefährden.

Stellschrauben gibt es hier einige: So kann festgelegt werden, dass das KI-System auf eigenen Servern operiert, damit keine weiteren Übermittlungen notwendig werden. Auch ist die Speicherdauer der aufgezeichneten Bilder mit Personenbezug auf das Nötigste zu begrenzen.

Kommt man zu dem Ergebnis, dass ein Einsatz einer KI-Videoüberwachung zulässig ist, gilt es noch mit den entsprechenden technischen-organisatorischen Maßnahmen (vgl. Art. 32 DS-GVO) das System zu sichern, beispielsweise durch verschlossene Serverräume, Zugriffskonzepte und Löschroutinen.

Sollen die Aufnahmen dazu verwendet werden, das KI-System weiter zu trainieren, muss auch hier im Einzelfall im Vorfeld nachvollzogen werden, wo und wie das Training erfolgt. Erfolgt das Training beispielsweise nicht nur für das eigene Bad auf den eigenen Servern, sondern beim Herstellerunternehmen und einem von diesem bereitgestellten Server, bedarf es auf Seiten der Badbetreiber_innen einer weiteren Rechtsgrundlage für die Übermittlung der Daten an das Herstellerunternehmen. Zeitgleich benötigt das Herstellerunternehmen eine eigene Rechtsgrundlage entsprechende Aufnahmen entgegenzunehmen und zu eigenen Zwecken zu verarbeiten.

Vor dem Hintergrund dieser komplexen datenschutzrechtlichen Prüfungen und des hohen finanziellen Einsatzes, der für die Einrichtung solcher Systeme erforderlich ist, empfehlen wir im Vorfeld der Einrichtung solcher Systeme unbedingt die eigenen Datenschutzbeauftragten zu konsultieren und bei Zweifelsfragen gerne auf uns zuzukommen.

☛ Weitere Informationen

Zu datenschutzrechtlichen Rechtgrundlagen bei KI-Anwendungen im Allgemeinen siehen unser Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz":
www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

DSK-Orientierungshilfe zur Videoüberwachung in Schwimmbädern:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/Orientierungshilfe-zur-Video%C3%BCberwachung-in-Schwimmb%C3%A4dern.pdf

Abteilung 3: Datenschutz im Gesundheits-, Sozial-, Bildungs- und Justizwesen

Team „Schule digital" sagt Ade: Drei Jahre Datenschutzarbeit an Schulen enden

✎ Art. 57 Abs. 1 Buchst. b), e), j) DS-GVO

Datenschutz an Schulen – viele haben davon gehört, aber nur wenige wissen, was das in der Praxis bedeutet und wie man ihn richtig umsetzt. Genau hier setzte das Team „Schule digital" an. Schon lange bietet der Landesbeauftragte für den Datenschutz seine Beratung an, doch mit der Gründung dieses Teams wurden Schulen gezielter unterstützt und fortgebildet.

Der Landtag von Baden-Württemberg erkannte die Herausforderungen und bewilligte großzügig drei Stellen, die von 2022 bis 2024 dafür sorgen sollten, das Thema Datenschutz in Schulen voranzutreiben. Diese Unterstützung ermöglichte dem Team „Schule digital", einiges zu leisten: In über 250 Fortbildungen wurden mehr als 4.400 Teilnehmende aus allen Bereichen des Schullebens erreicht – von Lehrkräften und Schulleitungen über Schulsekretariate bis hin zu Schülerinnen, Schülern und Eltern.

Gemeinsam mit dem Zentrum für Schulqualität und Lehrerbildung Baden-Württemberg (ZSL) entwickelte das Team umfassende Materialien zu den Grundlagen des Datenschutzes, die nun in landesweiten Lehrerfortbildungen zum Einsatz kommen. Bei einer mehrtägigen Veranstaltung wurden diese Unterlagen den Fortbildner_innen vorgestellt – eine Zusammenarbeit, die sich als erfolgreich erwies.

Doch das Team „Schule digital" ließ es nicht bei den Grundlagen bewenden. Es ging in die Tiefe und widmete sich den aktuellen, oft komplexen Datenschutzfragen, die Schulen heute herausfordern: Wie geht man mit der Nutzung privater Endgeräte um? Was muss bei elektronischen Tagebüchern beachtet werden? Welche technischen und organisatorischen Maßnahmen sind nötig, um den Datenschutz zu gewährleisten? Und – ganz aktuell – wie können Schulen den Datenschutz beim Einsatz von KI sicherstellen?

Ein weiterer Schritt war das Format „Datenschutzaufsicht meets Schulaufsicht". Das Team reiste zu allen vier Regierungspräsidien und vielen Staatlichen Schulämtern, um mit Schulreferentinnen und Schulreferenten sowie deren Leitungen unmittelbar ins Gespräch zu kommen. Auch auf Tagungen von Schulleitungen und Veranstaltungen von Lehrkräfteverbänden war das Team aktiv und brachte das wichtige Thema Datenschutz auf die Tagesordnung. Besonders wichtig war zudem die Sensibilisierung angehender Lehrkräfte an pädagogischen Hochschulen.

Ein echtes Highlight der letzten Jahre war die Teilnahme an der Bildungsmesse didacta 2024 (s. S. 85 f.). Der Messestand des Teams lockte viele Lehrkräfte, Schulleitungen und IT-Hersteller an, die für den Schulbereich tätig sind. Der Erfolg dieser Gespräche war so groß, dass auch die didacta 2025 in Stuttgart bereits fest eingeplant ist.

Doch so erfolgreich die letzten drei Jahre auch waren: Das Team „Schule digital" hat sich zum Jahresende nach Ablauf der Projektdauer verabschiedet. Wir danken dem Landtag noch einmal dafür, dass wir in den vergangenen drei Jahren durch die zeitlich befristete Finanzierung zusätzlicher Stellen Gelegenheit hatten, verstärkt für den Datenschutz an Schulen zu sensibilisieren und zahlreiche handelnde sowie betroffene Personen fortzubilden und weiterführendes Schulungsmaterial zu erarbeiten. Es war eine sehr gewinnbringende Zeit und es ist zu hoffen, dass an diese wertvollen Erfahrungen auf beiden Seiten auch in Zukunft angeknüpft werden kann.

Künstliche Intelligenz und Schule. Digital gezeichnet von Amalia, 11 Jahre.

KI in der Schule – ein rechtliches Risiko oder Pflicht für die Schulen?

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

Der Einsatz von Künstlicher Intelligenz in Schulen verspricht, das Lernen grundlegend zu verändern und individuelle Förderung zu erleichtern. Doch bleibt die Frage, inwieweit der Einsatz dieser Technologien – die durchaus auch erhebliche Risiken für die Rechte und Freiheiten der Schülerinnen und Schüler mit sich bringen können – rechtlich zulässig ist, vor allem im Hinblick auf Datenschutz und die Rechte der Lernenden.

Zwei große europäische Regelwerke sind hier entscheidend: die Datenschutz-Grundverordnung (DS-GVO) und die KI-Verordnung (KI-VO). Nach der DS-GVO müssen Schulen unter anderem bei automatisierten Entscheidungen sehr vorsichtig sein. Vor allem dürfen keine rechtlich relevanten Entscheidungen – wie zum Beispiel die Vergabe von Noten bei Klausuren und Prüfungen – ausschließlich auf Basis einer KI gefällt werden (vgl. Art. 22 DS-GVO). Sollte eine Korrektur zuerst durch eine KI erfolgen, ist außerdem zu beachten, dass bei menschlichen Entscheidenden die Tendenz besteht, die Ergebnisse des Computers ohne Kritik oder weitere Kontrolle zu übernehmen (sogenannter „Automation Bias").

In der KI-Verordnung stuft die EU Systeme, die Lernergebnisse bewerten, als „Hochrisiko-KI-Systeme" ein (Art. 6 Abs. 2 und 3 KI-VO in Verbindung mit Anhang III, Punkt 3 KI-VO). Das bedeutet, dass der Einsatz dieser Systeme strengen Vorschriften unterliegt. Schulen sollten daher schon deswegen vermeiden, KI-Systeme für Bewertungen oder Prüfungen einzusetzen, da damit ab August 2026 umfangreiche Pflichten verbunden sind. Ausdrücklich zu warnen ist davor, KI-Modelle mit allgemeinem Verwendungszweck (vgl. Art. 4 Nr. 63 KI-VO) zur Korrektur zu verwenden, da durch die Vornahme dieser speziellen Zweckbestimmung die Schule zum Anbieter des

KI-Systems werden kann (vgl. Art. 25 Abs. 1 Buchst. c) KI-VO), was sehr umfangreiche Pflichten nach sich zieht, die mit hohen Bußgeldern bewehrt sind.

Art. 22 Abs. 1 DS-GVO

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.

Art. 3 Nr. 63 KI-VO

„KIModell mit allgemeinem Verwendungszweck" ein KIModell – einschließlich der Fälle, in denen ein solches KIModell mit einer großen Datenmenge unter umfassender Selbstüberwachung trainiert wird –, das eine erhebliche allgemeine Verwendbarkeit aufweist und in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und das in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann, ausgenommen KIModelle, die vor ihrem Inverkehrbringen für Forschungs- und Entwicklungstätigkeiten oder die Konzipierung von Prototypen eingesetzt werden;

Art. 25 Abs. 1 KI-VO

In den folgenden Fällen gelten Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter eines Hochrisiko-KISystems für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Art. 16: wenn sie die Zweckbestimmung eines KISystems, einschließlich eines KISystems mit allgemeinem Verwendungszweck, das nicht als hochriskant eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, so verändern, dass das betreffende KISystem zu einem Hochrisiko-KISystem im Sinne von Art. 6 wird.

Ein weiterer kritischer Punkt: Der Umgang mit personenbezogenen Daten, insbesondere von Minderjährigen. Aktuell gibt es noch keine verlässlichen technischen Lösungen, die gewährleisten, dass die Rechte auf Auskunft, Berichtigung oder Löschung der Daten nach DS-GVO (vgl. Art. 15 – 17) bei KI-Systemen ausreichend umgesetzt werden können. Daher sollten Schulen auf keinen Fall Systeme einsetzen, die mit den personenbezogenen Daten ihrer Nutzerinnen und Nutzer trainieren.

Doch nicht jede Nutzung von KI in der Schule ist rechtlich problematisch. Wenn KI-Systeme nicht zur Bewertung eingesetzt werden, unterliegt ihr Einsatz keinen strengen Regulierungen der EU. Systeme, die das Lernen unterstützen, ohne die Lernenden zu bewerten, können also durchaus verwendet werden – mit einer wichtigen Ausnahme: Adaptive Lernsysteme, die den Lernprozess steuern, gelten ebenfalls als Hochrisiko-Systeme und sind daher auch streng reguliert (Anhang III, Punkt 3b KI-VO).

Allerdings benötigen die Nutzenden an den Schulen KI-Kompetenz (vgl. Art. 4 KI-VO): Ein ausreichendes Maß an Fähigkeiten, Kenntnisse, und das Verständnis, KI-Systeme sachkundig einzusetzen sowie sich der Chancen und Risiken von KI und möglicher Schäden, die sie verursachen kann, bewusst zu werden (vgl. Art. 3 Nr. 56 KI-VO). Unabhängig von diesem Passus der KI-Verordnung, welcher bereits ab Februar 2025 an den Schulen beim Einsatz von KI verpflichtend wird, ist dies für die Jugendlichen ein wichtiges Lernziel in unserer digitalisierten Welt.

Allerdings bedarf es für den Einsatz von KI-Systemen durch Schulen wegen der damit verbundenen Risiken und der zumindest potentiell erheblichen Eingriffstiefe in das Recht auf informationelle Selbstbestimmung auf Ebene des deutschen Verfassungsrechts in der Regel einer speziellen Ermächtigungsgrundlage. Die allgemeine Generalklausel, nach der personenbezogene Daten insoweit verarbeitet werden dürfen, als dies zur Aufgabenerfüllung erforderlich ist (vgl. § 4 LDSG), wird insoweit nicht ausreichen. Ohnehin sind Vorgaben des nationalen (Landes-)Rechts auch zu beachten, so z. B.

dass adaptive Lernsysteme gemäß § 115b Abs. 9 des Schulgesetzes nur „zum Zweck der technischen Unterstützung und Förderung des individuellen Lernwegs“ angewendet werden dürfen. Damit dürfen Lernergebnisse von Schülerinnen und Schülern in automatisierten, anpassungsfähigen Verfahren nach der Gesetzeslage beispielsweise weder zur Leistungsfeststellung bzw. -bewertung oder gar zur Notenbildung herangezogen werden; eine etwa erforderliche Prüfung des Leistungsstands der Schülerinnen und Schüler muss vielmehr auf andere Weise erfolgen.

Schließlich müssen Schulen, welche im Rahmen einer Auftragsdatenverarbeitung externe Systeme nutzen, wie bei allen digitalen Anwendungen, auch bei KI sicherstellen, dass keine personenbezogenen Daten für Zwecke des Anbieters verarbeitet werden. Eine Verarbeitung in Drittstaaten, die keine ausreichenden Datenschutzgarantien bieten, ist ebenfalls nicht zulässig (vgl. Kapitel V DS-GVO).

Der Einsatz von KI in der Schule ist also keineswegs unmöglich, jedoch mit rechtlichen Hürden verbunden. Insbesondere bei der automatisierten Bewertung von Klausuren oder der Verwendung adaptiver Systeme müssen Schulen äußerst vorsichtig sein. Für reine Lernunterstützungssysteme, die keine personenbezogenen Daten verarbeiten, sieht die Rechtslage dagegen entspannter aus. Klar ist: Die Zukunft des Lernens mit KI bietet spannende Chancen, doch nur wer die rechtlichen Rahmenbedingungen im Blick hat, kann diese auch gefahrlos nutzen.

Um die Schulen bei der rechtlichen Beurteilung der Nutzung von KI-Systemen zu unterstützen, bieten wir über unser Bildungszentrum Datenschutz und Informationsfreiheit (BIDIB) Fortbildungen an. Überdies haben wir hierzu wiederholt das Kultusministerium beraten.

© Illustration: Y. Dwiputri

☛ Weitere Informationen

Podcast Datenfreiheit – extra des LfDI BW zum Thema KI und Bildung:

Datenfreiheit: KI und Bildung an der Hochschule – Gespräch mit Rolf Schwartmann
tube.bawü.social/w/aSNXKRYqjsioPaCevDdrsA

Datenfreiheit: KI und Bildung an der Hochschule – Gespräch mit Tobias Seidl
tube.bawü.social/w/eB3NaJsQP9c12axRZbp1Fc

Datenfreiheit: KI und Bildung an der Schule – Gespräch mit Steffen Haschler
tube.bawü.social/w/k4qgnfyQYtz1M7qEeguMxC

KI und Bildung an der Schule – Gespräch mit Jan Wacke
tube.bawü.social/w/dAt6S3d7waV7MoLsBWxvnD

Datenpannen in der behördlichen Aufsichtspraxis

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

In der täglichen Arbeit kümmerte sich das Team des Landesdatenschutzbeauftragten um zahlreiche Meldungen von „Datenpannen“ der seiner Aufsicht unterliegenden datenschutzrechtlich Verantwortlichen. Fragen der Melde- und Benachrichtigungspflichten gehören weiterhin zu den Dauerbrennern in unserer behördlichen Aufsichtspraxis im Jahr 2024.

Nach Art. 33 Abs. 1 Satz 1 DS-GVO hat der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten diese unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, der gemäß Art. 55 DS-GVO zuständigen Aufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Pflichten natürlicher Personen führt. Nur wenn die Analyse des Vorfalls ergibt, dass die Verletzung voraussichtlich nicht zu einem Risiko führt, kann die Meldung an die Aufsichtsbehörde unterbleiben; auch in diesem Fall muss der Verantwortliche allerdings gemäß Art. 33 Abs. 5 DS-GVO die Verletzung des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang

stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen dokumentieren. Führt die Verletzung des Schutzes personenbezogener Daten dagegen sogar zu einem voraussichtlich hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, ist der Vorfall nicht nur der Aufsichtsbehörde zu melden, sondern sind darüber hinaus auch die betroffenen Personen nach Maßgabe des Art. 34 DS-GVO zu benachrichtigen.

Zur Bestimmung des Risikos wird der Verantwortlichen regelmäßig eine umfassende Prognoseentscheidung anstellen. Bei der Risikobeurteilung wird er sich von einer detaillierten Risikoidentifizierung leiten lassen, eine Einschätzung zur Eintrittswahrscheinlichkeit und Schwere möglicher Schäden vornehmen sowie abschließend das Risiko einer Risikostufe zuordnen.

Den Verantwortlichen trifft jedoch nicht nur eine Melde-, Benachrichtigungs- und Dokumentationspflicht nach den Art. 33 und 34 DS-GVO, sondern er hat den Vorfall auch zum Anlass zu nehmen, die von ihm getroffenen technischen und organisatorischen Maßnahmen dahingehend zu überprüfen, ob sie weiterhin gemäß Art. 24 und 25 DS-GVO ausreichend sind. Insbesondere müssen sie im angemessen Maße geeignet sein, künftig etwaige gleichgelagerte Verletzungen des Schutzes personenbezogener Daten zu vermeiden. Hierzu zählt, dass der Verantwortliche nach Art. 32 DS-GVO vor allem den Schutz der Daten vor Verlust, Schädigung und Missbrauch gewährleistet. Der jeweilige Einzelfall sowie die jeweilige Datenverarbeitung zeigen dabei auf, welche Maßnahmen erforderlich sind, um dieses Ziel zu erreichen.

Anhand des folgenden Falls, welcher uns als Aufsichtsbehörde gemäß Art. 33 DS-GVO gemeldet wurde, soll dies nochmals näher beleuchtet werden:

In der gynäkologischen Ambulanz eines Klinikums in Baden-Württemberg werden im Rahmen von ambulanten gynäkologischen Behandlungen Lichtbilder zur Wunddokumentation (und damit von intimsten Körperbereiche von Patientinnen) mittels einer Digitalkamera angefertigt. Um eine Verwechslung der behandelten Patientinnen zu verhindern, wurde mit den Lichtbildaufnahmen ein Etikett abfotografiert, das die Stammdaten (Vor- und Nachname) der betroffenen Patientinnen ausweist und so eine Zuordnung zur behandelten Patientin ermöglicht. Am Ende des Behandlungstages wurden die Fotos digitalisiert und der jeweiligen Patientinnenakte zugewiesen.

Eines Tages wurde von Beschäftigten der betroffenen Abteilung festgestellt, dass sich ebendiese Digitalkamera nicht an dem ihr zugewiesenen Ort befand. Die Beschäftigten haben daraufhin eine umfassende Suche nach der Hardware veranlasst, bevor sie das Gerät als endgültig verloren erklärten und den Verlust dem Klinikvorstand und unter anderem der Datenschutzbeauftragten meldeten. Wie sich herausstellte, war die Digitalkamera am Vorabend, entgegen der verbindlichen Regelung zur Wunddokumentation, nicht in den abschließbaren Schrank verbracht worden, sondern befand sich nach den Behandlungen noch in dem abgeschlossenen Untersuchungsraum. Für die Nutzung der Digitalkamera ist beim Verantwortlichen ein Regelprozess definiert, der das Wegschließen der Digitalkamera nach erfolgter Nutzung vorgibt. Dieser Prozess wurde demnach durchbrochen.

Der Verantwortliche bewertete das Risiko richtigerweise als hoch und benachrichtigte die Betroffenen von der Verletzung des Schutzes personenbezogener Daten nach Art. 34 DS-GVO.

Im Rahmen der Aufklärung dieser Datenpanne arbeitete der Verantwortliche kooperativ mit der Aufsichtsbehörde zusammen. Unsererseits wurden insbesondere die technischen und organisatorischen Maßnahmen abgefragt und mit Blick auf Art. 24, 25 und 32 DS-GVO Prozessanpassungen diskutiert, um Datenschutzverletzungen dieser Art künftig zu verhindern.

Hinsichtlich des Zugriffs- und Berechtigungskonzepts meldete uns der Verantwortlichen zurück, dass künftig – in Abkehr zur vorhergehenden „Schlüssel-Schloss-Praxis“ hin zur noch qualitativeren Umsetzung einer Schlüsselregelung – ein Schlüsselkasten mit einem Zahlenschloss etabliert werden soll. Die Zahlenkombination soll nur dem berechtigten Personal offengelegt werden und nur

diesem Personal einen Zugriff auf die Digitalkamera ermöglichen. Empfehlenswert aus unserer Sicht erscheint bei der Umsetzung von Zugriffs- und Berechtigungskonzepten zudem die Führung einer Berechtigungsdokumentation, um binnen kürzester Zeit nachvollziehen zu können, wer über die Digitalkamera zuletzt verfügte.

Neben der Frage der Sicherung der Hardware erschloss sich uns außerdem nicht, weshalb die konkreten Patientenstammdaten auf einem Etikett an die Bilddatei niedergeschrieben werden mussten. Wir verkennen dabei nicht, dass eine Patientenverwechslung unter allen Umständen ausgeschlossen werden muss. Nach unserer Ansicht dürften jedoch pseudonymisierte Daten ausreichen, um die Lichtbilder trennscharf zu bezeichnen und so eine Verwechslung des intimen Bildmaterials vollständig auszuschließen. Ein Personenbezug wäre dann nur unter Heranziehung weitergehender Informationen möglich, was einem Missbrauch vorbeugen würde. Ausreichend wären etwa sog. „sprechende Namen" oder „Patienten-ID" mit Datum / Uhrzeit. Einer Patientinnenverwechslung hätte auch dadurch begegnet werden können, dass unmittelbar nach jeder Wunddokumentation die Bilder in das Krankenhausinformationssystem („KIS") zur jeweils behandelten Patientin überführt werden und der unmittelbare Personenbezug nicht bereits auf der Digitalkamera, sondern erst im technisch gesicherten Bereich hergestellt wird. Eine Verschärfung der internen Prozesse beim Verantwortlichen wurde letztlich dahingehend erzielt, dass die Lichtbilder von der Digitalkamera unverzüglich nach der Aufnahme und damit nach jeder Behandlung ins „KIS" überführt werden und nach erfolgreicher Übertragung umgehend und endgültig von der Digitalkamera gelöscht werden. Hierzu gehört auch eine Formatierung des Speichermediums (Speicherkarte) und nicht nur die Freigabe des Speicherplatzes als solchen.

Aus der behördlichen Aufsichtspraxis lässt sich anhand des dargestellten Sachverhalts sehr gut veranschaulichen, dass die Nachteile für die Betroffenen aus der Verletzung des Schutzes personenbezogener Daten bei besonderen Kategorien i. S. v. Art. 9 DS-GVO, also insbesondere bei Gesundheitsdaten gemäß Art. 4 Ziff. 15 DS-GVO, regelmäßig sehr schwer wiegen. Hier gilt es nicht nur Betroffene frühzeitig über die Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, sondern auch besonders, die internen Prozesse einer kritischen Prüfung zu unterziehen und technische und organisatorische Maßnahmen nachzujustieren bzw. neu zu implementieren, um vergleichbare Datenpannen künftig auszuschließen.

Für den Umgang mit Datenpannen insbesondere in den Bereichen Wirtschaft und Gesundheitswesen wird das hohe Schulungsbedürfnis der Verantwortlichen erkannt. Nicht zuletzt deshalb erfreute sich die Schulung „Grundlagen des Datenpannen-Managements" in unserem hauseigenen Bildungszentrum für Datenschutz und Informationsfreiheit (BIDIB) im Jahr 2024 einer sehr großen Beliebtheit. Weitere Veranstaltungen für das Jahr 2025 sind bereits geplant.

☛ Weitere Informationen

Unser Bildungsangebot finden Sie abrufbar unter: www.baden-wuerttemberg.datenschutz.de/bildungszentrum.

Inhalt des Handelsregisters: Nachbesserung des Gesetzes und Änderung einer Dienstordnung

✎ Art. 57 Abs. 1 Buchst. d) – f) DS-GVO

Im 38. Tätigkeitsbericht für das Jahr 2022 hatten wir uns zur seit dem 1. August 2022 kostenfreien und ohne Registrierung möglichen Einsicht in das Handelsregister geäußert (9.1.1, Seite 51). Wir hatten unter anderem darauf hingewiesen, dass die vereinfachte und kostenfreie Zugangsmöglichkeit bei vielen Betroffenen die Sorge um einen Missbrauch ihrer Daten ausgelöst habe – z. B. in Fällen, in denen in den abrufbaren Dokumenten die vollständigen Wohnanschriften oder etwa Erbscheine und Erbverträge enthalten sind. Hierzu erreichten uns auch im Jahr 2024 entsprechende Eingaben.

Angesichts der einfachen und kostenfreien Möglichkeit, personenbezogene Daten aus dem Handelsregister abzurufen, ist es von besonderer Bedeutung, dass sich die Aufnahme von Dokumenten zur unbeschränkten Einsicht auf solche Dokumen-

te bzw. personenbezogene Daten beschränkt, die für den Rechtsverkehr erforderlich sind.

Um dies sicherzustellen, wurden bereits im Dezember 2022 die Vorschriften des § 9 Abs. 1 Satz 2 und des § 9 Abs. 7 in die Handelsregisterverordnung (HRV) eingefügt.

In § 9 Abs. 1 Satz 2 Halbsatz 1 HRV ist nun geregelt, dass unter den in den Registerordner aufzunehmenden Dokumenten solche zu verstehen sind, deren Einreichung durch besondere (handels-) rechtliche Vorschriften angeordnet ist. Zudem wird in § 9 Abs. 2 Satz 2 Halbsatz 2 HRV nun klargestellt, dass Dokumente, deren Einreichung nicht durch besondere Rechtsvorschriften angeordnet ist, aber im Registerverfahren entweder auf Anforderung des Registergerichts oder überobligatorisch eingereicht werden, grundsätzlich nicht in den Registerordner aufgenommen werden sollen. Hierbei handelt es sich etwa um Erbnachweise, wie z. B. Erbscheine, Erbverträge und öffentliche Testamente, die nach § 12 Abs. 1 Satz 5 des Handelsgesetzbuchs zum Nachweis der Rechtsnachfolge eingereicht werden.

Sofern in einer dem Registergericht eingereichten Datei neben Dokumenten, deren Einreichung durch Rechtsvorschrift besonders angeordnet ist, auch Dokumente enthalten sind, deren Einreichung nicht besonders angeordnet ist, kann das Registergericht jedoch grundsätzlich alle in dieser Datei enthaltenen Dokumente in den Registerordner einstellen. Es liegt somit auch in der Verantwortung der einreichenden Stellen, Dokumente gegebenenfalls in gesonderten Dateien einzureichen, um zu verhindern, dass personenbezogene Daten „unnötigerweise“ zum Abruf bereitstehen.

In § 9 Abs. 7 HRV wird nun geregelt, dass und wie in Ausnahmefällen ein Austausch von Dokumenten erfolgen kann. Sind in einem ursprünglich eingereichten Dokument teilweise Angaben enthalten, die nicht in den Registerordner gehören, kann ein neu eingereichtes Dokument in den Registerordner eingestellt werden, welches nur die für den Rechtsverkehr erforderlichen Angaben enthält. Ein solcher Austausch ist kenntlich zu machen und das Datum der Aufnahme des alten Dokuments in den Registerordner anzugeben. Auf diese Weise wird darüber informiert, dass das ausgetauschte Dokument ein ursprüngliches Dokument ersetzt.

Am 1. Juni 2023 ist außerdem in sämtlichen Bundesländern eine Änderung der Dienstordnung der Notarinnen und Notare (DONot) in Kraft getreten, die die Vorschriften zur Bezeichnung von Beteiligten in notariellen Urkunden und die elektronische Übermittlung von Dokumenten an Registergerichte betreffen. Die Änderungen finden sich in den neu angepassten Bestimmungen des § 5 Abs. 1 DONot und im neu eingefügten § 5a DONot.

In § 5 Abs. 1 Satz 4 DONot n. F. ist z. B. vorgesehen, dass generell von der Angabe einer Anschrift abgesehen werden kann, wenn die Urkunde zur Übermittlung an ein Registergericht bestimmt ist sowie Zweifel und Verwechslungen ausgeschlossen sind.

Nach § 5 Abs. 1 Satz 5 DONot n. F. kann nun bei sämtlichen natürlichen Personen, die geschäftlich oder dienstlich auftreten, anstelle von Wohnort und Anschrift eine Geschäfts- bzw. Dienstanschrift einschließlich des Ortes angegeben werden.

Im neu eingefügten § 5a DONot ist geregelt, dass Notarinnen und Notare bei einer elektronischen Übermittlung von Dokumenten in öffentlich beglaubigter Form an das Registergericht Wohnanschriften, Seriennummern von Ausweisdokumenten sowie Kontoverbindungen entweder nicht in die Urkunde aufnehmen oder vor einer Übermittlung unkenntlich machen sollen. Gemäß § 5a Satz 2 DONot n. F. gilt dies nicht, wenn der Entwurf des Dokumentes nicht von der übermittelnden Notarin oder dem übermittelnden Notar gefertigt wurde.

Die vorgenannten Änderungen und Klarstellungen könnten wesentlich dazu beitragen, dass künftig nur solche personenbezogenen Daten in den Registerordner eingestellt und damit im Handelsregister abgerufen werden können, die für den Rechtsverkehr erforderlich sind. Ob dies tatsächlich gelingt, hängt – wie den vorstehenden Ausführungen zu entnehmen ist – jedoch auch ganz entscheidend davon ab, in welcher Form und mit welchem Inhalt Dokumente zum Handelsregister eingereicht werden.

Krankenhaussterben und der Schutz von Patientendaten

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

In einem Krankenhaus werden täglich eine Vielzahl an Gesundheitsdaten verarbeitet. Wichtig dabei ist, dass die Sicherungsmaßnahmen dieser besonders schutzbedürftigen Kategorie personenbezogener Daten im Sinne von Art. 9 DS-GVO den Anforderungen des Datenschutzes genügen, und zwar auch nach Schließung oder Insolvenz von Krankenhäusern.

Leider wird dieser Schutz sensibler Patientendaten indes häufig nicht über die Schließung eines Krankenhauses hinaus aufrechterhalten. Teilweise gerät mit der Schließung des Krankenhauses die Verantwortung für die weitere Speicherung und ggf. ordnungsgemäße Löschung sowie für die Erfüllung von Betroffenenrechten in Vergessenheit – oder die Verantwortung wird sonst aus Nachlässigkeit oder mangels unmittelbaren Eigeninteresses des Verantwortlichen an der Wahrung der Reputation nicht mehr wahrgenommen. Oder es werden – insbesondere im Falle der Insolvenz des Krankenhauses – die Kosten hierfür nicht mehr aufgebracht. Wiederholt wurden die Datenschutzaufsichtsbehörden mit Fällen der Schließung von Krankenhäusern konfrontiert, in denen eine sichere Aufbewahrung und der Zugang der Betroffenen zu den Patientendaten nicht gewährleistet waren. Teilweise bestand sogar die Gefahr, dass sich Unbefugte Zugang zu den Krankenakten verschaffen konnten (über einen solchen Fall – ein Krankenhaus als „lost place" – aus Baden-Württemberg berichteten wir beispielsweise in unserem 37. Tätigkeitsbericht Datenschutz).

Bereits zu Beginn des Jahre 2024 hatte angesichts der verarbeiteten Sorge um die Finanzierung von Krankenhäusern die Berichterstattung zu einem zu befürchtenden Krankenhaussterben stark zugenommen, und auch in der Zukunft ist weiterhin mit der Schließung einer erheblichen Zahl von Krankenhäusern zu rechnen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) nahm diesen Umstand mit Sorge zur Kenntnis und beauftragte deswegen den Arbeitskreis Gesundheit und Soziales mit dem Entwurf eines Entschließungspapiers. Im Auftrag der DSK beteiligten wir uns gemeinsam mit anderen Datenschutzaufsichtsbehörden aktiv an der Erstellung des Positionspapiers. Dabei konnten wir darauf hinweisen, dass es in der Gesetzgebung Baden-Württembergs teilweise schon einzelne gute Lösungsansätze für (niedergelassene) Heilberufe gibt: In § 4 Abs. 1 Satz 3

Wird ein Krankenhaus geschlossen, leeren sich die Flure. Sensible Patientendaten sollten nicht liegen bleiben.

des Heilberufekammergesetzes haben die Kammern Patientenunterlagen für die Dauer der Aufbewahrungspflicht in Obhut zu nehmen und den Patient_innen Einsicht zu gestatten, sofern dies nicht durch das verpflichtete Kammermitglied oder dessen Rechtsnachfolgerin oder -nachfolger gewährleistet ist.

Für Krankenhäuser jedoch fehlt es nach wie vor auch in Baden-Württemberg an einer hinreichenden Lösung der Problematik. Gegenüber dem Sozialministerium haben wir in einer Stellungnahme zum Reformbedarf des Landeskrankenhausgesetzes darauf hingewiesen, dass auch in Baden-Württemberg hier die hohe Notwendigkeit einer Regelung besteht. Die in der Entschließung der DSK beispielhaft angeführten Regelungen anderer Länder zeigen hierzu Lösungsmöglichkeiten auf. So wird in anderen Ländern etwa den Krankenhäusern die Obliegenheit auferlegt, der Krankenhaus-Aufsicht Konzepte zur weiteren Verwahrung der Patientenakten einschließlich der Befriedigung von Betroffenenrechten für den Fall der Insolvenz und der Schließung des Krankenhauses zur Prüfung vorzulegen, und die Schaffung eines obligatorischen Patientenaktensicherungsfonds angeordnet.

Gerade angesichts der aktuellen Krankenhausfinanzierungsproblematik ist regulatorische und faktische Vorsorge zu treffen für die Sicherung der ordnungsgemäßen Speicherung und Löschung von Patient_innenakten sowie die Erfüllung von Betroffenenrechten, wenn Krankenhäuser geschlossen oder gar ihre Träger insolvent werden. Hier besteht auch in Baden-Württemberg ein dringender Regelungsbedarf.

☛ Weitere Informationen

Entschließung „Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern" der DSK vom 15.05.2024:
datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf

37. Tätigkeitsbericht Datenschutz 2021 des LfDI BW, Lost places, S. 94 f.: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf

Unwetter und Datenschutz – ein unerwarteter Zusammenhang

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

Wer würde schon vermuten, dass ein starkes Unwetter und der Datenschutz etwas miteinander zu tun haben könnten? Doch genau diese unerwartete Verbindung wurde uns auf lebhafte Weise vor Augen geführt.

Nach heftigen Regenfällen verwandelte sich ein normalerweise harmloser Bach in einer kleinen Gemeinde in einen reißenden Strom. Innerhalb weniger Stunden wurden zahlreiche Keller geflutet – auch der Keller einer örtlichen Schule. Das massive Naturereignis entpuppte sich schnell auch als Datenschutz-Problem. Denn in diesem Keller lagerten die Abschriften der Abschlusszeugnisse der letzten Jahre. Diese Zeugnisse sind mehr als nur Papier; sie sind der Schlüssel für viele Ehemalige, die im Verlustfall darauf angewiesen sind, dass sie von der Schule Abschriften erhalten.

Das Unwetter machte vor diesen wichtigen Dokumenten keinen Halt. Der Keller wurde nicht nur geflutet, sondern auch mit Schlamm überzogen, wodurch die wertvollen Abschriften nahezu vollständig zerstört wurden. So meldete die Schule uns eine Datenpanne nach Art. 33 DS-GVO. Die personenbezogenen Daten, die in diesen Zeugnissen steckten, waren plötzlich nicht mehr verfügbar.

Wir forderten die Schule auf, alles zu tun, um die beschädigten Dokumente zu retten. Doch die Bemühungen blieben weitgehend erfolglos. Da hier ein hohes Risiko für die Rechte der Betroffenen besteht – insbesondere, wenn eine für eine Bewerbung notwendige Abschrift aufgrund des Ereignisses nicht mehr beschafft werden kann, weil das Originalzeugnis verloren ging – hielten wir eine Benachrichtigung der betroffenen Personen gemäß Art. 34 DS-GVO grundsätzlich für erforderlich. Da wegen deren Vielzahl aber nicht jede Person einzeln benachrichtigt werden konnte, schlugen wir der Schule vor, gemäß Art. 34 Abs. 3 Buchst. c) DS-GVO eine öffentliche Bekanntmachung über die Presse, etwa im Amtsblatt der Gemeinde, vorzunehmen. Dem Vorschlag kam die Schule nach – in

dem Bestreben zu erreichen, dass die betroffenen Personen in dieser unvorhersehbaren unglücklichen Situation zumindest soweit möglich informiert sind.

Auch die Verfügbarkeit personenbezogener Daten, die noch benötigt werden, stellt ein Datenschutzthema dar. Daten, die noch benötigt werden, dürfen auch nicht verloren gehen.

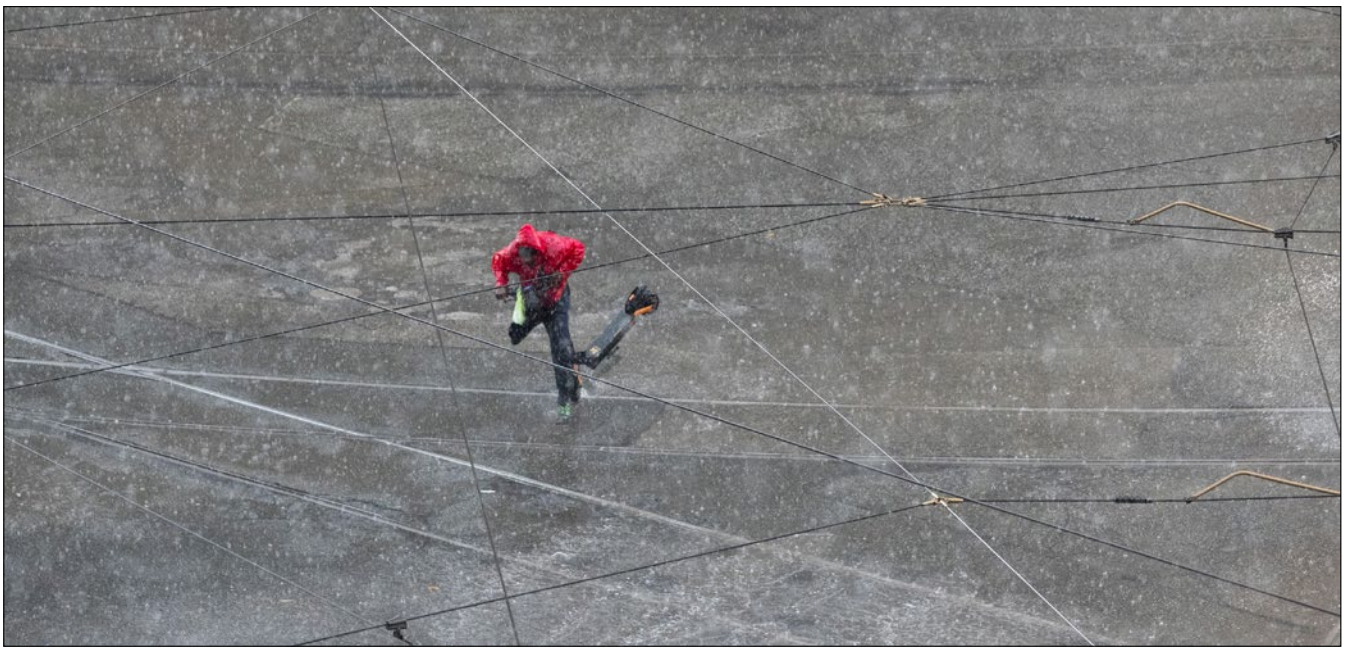
Datenschutz und Informationsfreiheit zusammen: Über den Zugang zu Aufzeichnungen über die Verwendung von Pflanzenschutzmitteln

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

Ein Fall aus der Praxis, der auch aus einem Lehrbuch stammen könnte: Es geht um das Zusammenspiel von europäischem und nationalem Recht und das Verhältnis von Datenschutz und Informationsfreiheit.

Die Zugänglichmachung von Aufzeichnungen über die Verwendung von Pflanzenschutzmitteln stößt seit geraumer Zeit auf großes öffentliches Interesse. Im Januar 2024 wurden bundesweit die aktuellsten Aufzeichnungen über die berufliche Anwendung von Pflanzenschutzmittel im Sinne des § 11 Abs. 1 Pflanzenschutzgesetz bzw. des Art. 67 Abs. 1 UnterAbs. 1 Satz 2 der EU-Pflanzenschutz-Verordnung bei den jeweiligen Aufsichtsbehörden über die Plattform FragDenStaat angefragt. Zu den (umwelt-) informationspflichtigen Stellen zählen unter anderem auch die Landratsämter in Baden-Württemberg. Der Verwaltungsgerichtshof Baden-Württemberg hatte bereits im Mai 2021 mit fünf Urteilen entschieden, dass das Land Baden-Württemberg grundsätzlich Zugang zu Informationen über die von den Landwirten geführten Aufzeichnungen gewähren muss (VGH 10. Senat vom 4. Mai 2021 – 10 S 1348 / 20).

Sowohl Landtagsabgeordnete als auch die von diesen neueren Anfragen insbesondere drittbetroffenen Landwirte, deren Aufzeichnungen zugänglich gemacht werden sollten, wandten sich mit der Sorge an uns, der Schutz ihrer personenbezogenen Daten werde in diesen Zugangsverfahren nicht hinreichend gewährleistet. Hierbei spielt insbesondere auch eine Rolle, dass die landwirtschaftlichen Betriebe oft als Einzelunternehmen geführt werden, bei welcher der Vor-und Zuname des Betroffenen als Einzelkaufmann nicht vom landwirtschaftlichen Betrieb abtrennbar ist.



Das Wetter hat etwas mit Datenschutz zu tun? Wir waren auch überrascht, aber ja: das kann ausnahmsweise sein.

Beim Zugang zu Daten, insbesondere von personenbezogenen Daten, stellt sich die Frage, auf Basis welcher Rechtsgrundlage dieser erfolgen kann oder nicht erfolgen darf. Hierbei sind sowohl europäische als auch nationale Regelungen zu beachten.

Der Data Governance Act (DGA) (EU 2022 / 868) ist Teil der EU-Datenstrategie 2020, die zum Ziel hat, einen Binnenmarkt für Daten in der EU zu schaffen und den Austausch von Daten gesetzeskonform zu ermöglichen und zu erleichtern. Geschützte Datensätze, die von öffentlichen Stellen im Rahmen ihrer Tätigkeit erhoben werden, sollen rechtssicher und ortsunabhängig verfügbar gemacht werden können. Die zugrundeliegende Vision sieht einen zukünftigen Datenzugang für alle und einen Abbau der digitalen Zugangskluft vor. Die von datenaltruistischen Organisationen zur Verfügung gestellten Daten sollen vertrauenswürdig und sicher geteilt und vor allem weiterverwendet werden können. Besonders in ausgesuchten Forschungsgebieten kann die einwilligungsbasierte, gemeinsame Nutzung von Daten die Gewinnung neuer Erkenntnisse und die Entwicklung neuer Verfahren vorantreiben. Der DGA schafft keine (neue) Rechtsgrundlage für den Austausch personenbezogener Daten. Sämtliche Rechtsakte sind neben dem DGA anwendbar oder gehen ihm vor, wie z. B. die DS-GVO. Auf Basis des DGA kommt daher ein Zugang nicht in Betracht, da die Daten zwar von öffentlichen Stellen erhoben werden, jedoch nicht von datenaltruistischen Organisationen gemäß DS-GVO einwilligungsbasiert zur Verfügung gestellt werden.

Der Zugang zu Umweltinformationen über Emissionen in Form von Aufzeichnungen über Pflanzenschutzmittel ist im Ergebnis aber dennoch ohne Rücksicht darauf zu erteilen, ob die begehrten Informationen personenbezogene Daten der aufzeichnenden Person umfassen. Dies ergibt sich aus nachfolgenden Erwägungen:

Das Landesinformationsfreiheitsgesetz (LIFG) regelt den Zugang zu allgemeinen amtlichen Informationen, das Umweltverwaltungsgesetz (UVwG) bietet einen spezielleren Zugang zu Umweltinformationen. Der Anspruch auf Zugang zu Umweltinformationen ist umfassender, und die gegenüber diesem Anspruch einwendbaren Schutzgründe sind sehr viel eingeschränkter als beim Anspruch auf Informationszugang aus dem Landesinformationsfreiheitsgesetz.

Die Verwendung von Pflanzenschutzmitteln kann Datenschutz und Informationsfreiheit zugleich tangieren.

Soweit Aufzeichnungen zur beruflichen Anwendung von Pflanzenschutzmitteln bei einer Verwaltungsbehörde zu dienstlichen Zwecken vorhanden sind, handelt es sich um amtliche Informationen im Sinne des § 3 Nr. 2 LIFG, zu denen nach den Vorgaben des Landesinformationsfreiheitsgesetzes auf Antrag der Zugang zu gewähren ist. Der Anspruch auf Zugang zu amtlichen Informationen ist auch dann an sich nicht ausgeschlossen, wenn es sich bei den amtlichen Informationen zugleich um Umweltinformationen im Sinne des Umweltverwaltungsgesetzes (s. § 23 Abs. 3 UVwG) handelt. Denn das Umweltverwaltungsgesetz regelt den Zugang zu Umweltinformationen ausdrücklich nicht abschließend (s. § 24 Abs. 1 Satz 2 UVwG), so dass der Anspruch aus dem Landesinformationsfreiheitsgesetz daneben besteht (vgl. § 1 Abs. 3 LIFG). Der Anspruch auf amtliche Informationen nach dem Landesinformationsfreiheitsgesetz ist jedoch durch ein Abwägungserfordernis begrenzt, soweit die amtlichen Informationen zugleich personenbezogene Daten darstellen (hier: soweit die Informationen über die Aufzeichnungen zur beruflichen Anwendung von Pflanzenschutzmitteln sich auf eine natürliche Person beziehen lassen, die die Pflanzenschutzmittel beruflich angewendet hat): Willigt die betroffene Person in dieser Konstellation nicht in die Gewährung des Zugangs ein, darf die Behörde, die auf Zugang zu den bei ihr vorhandenen amtlichen Informationen in Anspruch genommen wird, den Zugang nur gewähren, soweit im konkreten Fall das Informationsinteresse an der Bekanntgabe das schutzwürdige Interesse der betroffenen Person am Ausschluss der Information überwiegt (§ 7 Abs. 1 LIFG).

Dieser Abwägung ist die Behörde allerdings in bestimmten Fällen enthoben, soweit sich der Anspruch auf Informationszugang auf das Umweltverwaltungsgesetz stützen lässt: Wenn Aufzeichnungen über die berufliche Anwendung von Pflanzenschutzmitteln nach Art. 67 Abs. 1 Satz 2 der EU-Pflanzenschutz-Verordnung verlangt werden, stellen die Informationen, zu denen der Zugang gewährt werden soll, nicht nur allgemein amtliche Informationen dar, in Bezug auf die sich das Zugangsrecht aus dem Landesinformationsfreiheitsgesetz ergibt, sondern zugleich Umweltinformationen, deren Zugang in Baden-Württemberg in § 24 UVwG geregelt ist. Umweltinformationen sind nämlich in § 23 Abs. 3 UVwG definiert. Umweltinformationen sind danach insbesondere Daten über Maßnahmen oder Tätigkeiten, die sich auf Umweltbestandteile (z. B. Luft, Wasser, Boden, Artenvielfalt) mindestens wahrscheinlich auswirken (s. § 23 Abs. 3 Nummer 3 Buchst. a) UVwG). Hierbei genügt die Möglichkeit einer Beeinträchtigung von Umweltbestandteilen. Davon ist bei der beruflichen Anwendung von Pflanzenschutzmitteln auszugehen.

Gemäß § 24 Abs. 1 Satz 1 UVwG hat jede Person nach Maßgabe dieses Gesetzes Anspruch auf freien Zugang zu Umweltinformationen, über die eine informationspflichtige Stelle im Sinne von § 23 Abs. 1 UVwG verfügt, ohne ein rechtliches Interesse darlegen zu müssen. Der durch § 24 Abs. 1 Satz 1 UVwG demnach an sich voraussetzungslos gewährleistete Zugang zu Umweltinformationen ist allerdings (vergleichbar mit der Regelung im Landesinformationsfreiheitsgesetz) im Allgemeinen zum Zwecke des Schutzes personenbezogener Daten nach § 29 UVwG beschränkt: Nach § 29 Abs. 1 Satz Nummer 1 UVwG ist der Antrag auf Zugang zu Umweltinformationen grundsätzlich abzulehnen, soweit durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch Interessen der betroffenen Person erheblich beeinträchtigt würden, es sei denn, die betroffenen Personen haben eingewilligt oder das öffentliche Interesse an der Bekanntgabe überwiegt.

In Satz 2 der Norm des § 29 Abs. 1 UVwG ist jedoch abweichend hiervon geregelt, dass der Zugang zu Umweltinformationen über Emissionen nicht unter Berufung auf die in Satz 1 Nummer 1 genannten Gründen (also insbesondere nicht mit Blick auf den Schutz personenbezogener Daten) abgelehnt werden kann. Das heißt, dass im Falle des Zugangs zu Informationen über Emissionen keine einzelfallbezogene Abwägung zwischen dem Recht auf informationelle Selbstbestimmung und dem öffentlichen Interesse auf Zugang stattfindet. Der Gesetzgeber hat hier eine Vorrangentscheidung zugunsten der Bekanntgabe der personenbezogenen Daten bereits selbst getroffen (HK-IZR

BW / Anja Hentschel, 1. Aufl. 2017, UVwG § 28 Rn. 36, beck-online, so auch VGH Baden-Württemberg, Urteil vom 04.05.2021 – 10 S 2422 / 20).

Der EuGH hat im Vorabentscheidungsersuchen vom 23.11.2016 (EuGH, 23.11.2016, C-442 / 14) festgestellt, dass das Freisetzen von Produkten oder Stoffen wie Pflanzenschutzmitteln oder Biozid-Produkten, und in diesen Produkten enthaltenen Stoffen in die Umwelt dem Begriff „Emissionen in die Umwelt" unterfällt (so auch der VGH Baden-Württemberg, Urteil vom 04.05.2021 – 10 S 2422 / 20). Demnach handelt es sich bei solchen Aufzeichnungen um Umweltinformationen über Emissionen.

Dem Ergebnis, dass der Zugang zu den Umweltinformationen über Emissionen gemäß § 29 Abs. 1 Satz 2 UVwG auch dann zu gewähren ist, wenn durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch Interessen der betroffenen Personen erheblich beeinträchtigt werden, steht auch nicht der Umstand entgegen, dass nach § 11 Abs. 3 des Pflanzenschutzgesetzes (PflSchG) die Behörde nur bei Vorliegen eines berechtigten Interesses und unter Wahrung der Betriebs- und Geschäftsgeheimnisse des Aufzeichnenden im Einzelfall Auskunft über die von der Europäischen Pflanzenschutzmittelverordnung vorgeschriebenen Aufzeichnungen gewähren soll. Denn es würde nach den Ausführungen des VGH Baden-Württemberg in der angeführten Entscheidung den Vorgaben der Europäischen Vorgaben der Umweltinformationsrichtlinie widersprechen, wenn man § 11 Abs.3 PflSchG als abschließende Regelung des Informationszugangs ansehen würde. Deswegen bleibe der Anspruch aus § 24 Abs. 1 Satz 1 UVwG neben § 11 Abs. 3 PflSchG anwendbar.

Der Zugang zu Umweltinformationen über Emissionen in Form von Aufzeichnungen über Pflanzenschutzmittel ist daher ohne Rücksicht darauf zu erteilen, ob die begehrten Informationen personenbezogene Daten der aufzeichnenden Person umfassen. Da sich dieses Ergebnis schon aus dem speziellen Anspruch aus § 24 Abs. 1 Satz 1 UVwG ergibt, kann dahinstehen, ob die Behörde auch in Bezug auf den Anspruch aus § 1 Abs. 2 LIFG bei ihrer Ermessensausübung nach § 5 Abs. 1 LIFG die gesetzliche Wertung aus § 29 Abs. 1 Satz 2 UVG berücksichtigen müsste.

☛ Weitere Informationen

Aktueller Situationsbericht des Deutschen Bauernverbands
situationsbericht.de/3/34-betriebs-und-rechtsformen

VGH Baden-Württemberg, Beschluss vom 13.12.2019 – 10 S 2614 / 19, Rn. 15 ff.: www.landesrecht-bw.de/bsbw/document/NJRE001409436

Auskunft beim Arzt

✎ Art. 57 Abs. 1 Buchst. a) – g) DS-GVO

Die Datenschutz-Grundverordnung regelt mehrere sogenannte Betroffenenrechte. Hierbei handelt es sich um Ansprüche und Gestaltungsmöglichkeiten der betroffenen Person. Zentrales Betroffenenrecht ist das Auskunftsrecht nach Art. 15 DS-GVO. Dieses spiegelt sich auch in unserer aufsichtsrechtlichen Praxis wider. Im vergangenen Berichtszeitraum haben sich zahlreiche Personen mit dem Vortrag an uns gewandt, dass ihrem Verlangen nach Auskunft nicht oder nur unzureichend nachgekommen worden sei. Teilweise war es hier sachdienlich, die sich an uns wendenden Personen zu beraten, wie sie ein korrektes Auskunftsersuchen stellen. In anderen Fällen haben wir uns an die Verantwortlichen gewandt mit dem Ziel, eine Auskunftserteilung zu ermöglichen.

Art. 15 DS-GVO gewährt der betroffenen Person das Recht auf Auskunft über die sie betreffenden personenbezogenen Daten, die der Verantwortliche verarbeitet. Dieses Recht umfasst auch ein Recht auf Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind.

Im Bereich der Ärzte und Zahnärztinnen hat der Europäische Gerichtshof (EuGH) mit seinem Urteil vom 26. Oktober 2023, Az. C 307 / 22, den Zugang zu Patientenakten gestärkt und unsere bisherige Aufsichtspraxis bestätigt.

Der EuGH hat in diesem Urteil zunächst entschieden, dass die Verpflichtung des Verantwortlichen, der betroffenen Person unentgeltlich eine erste Kopie ihrer personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen, auch dann gelte, wenn der betreffende Antrag mit anderen als den in Satz 1 des 63. Erwägungsgrundes der DS-GVO genannten Zwecken begründet werde. In Erwägungsgrund 63 steht, dass die betroffene Person ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten besitzt und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können sollte, „um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit prüfen zu können". In dem Gerichtsverfahren vor dem EuGH zugrundeliegenden Fall hatte die die Auskunft verlangende Person eine Kopie ihrer Patientenakte verlangt, um Haftungsansprüche gegen den behandelnden Arzt geltend zu machen. Der EuGH hat hier festgestellt, dass die Ausübung des Auskunftsrechts nicht von Bedingungen abhängig gemacht werden dürfe, die der Unionsgesetzgeber nicht ausdrücklich festgelegt habe, wie etwa von der Verpflichtung, einen der im ersten Satz des 63. Erwägungsgrundes der DS-GVO genannten Gründe geltend zu machen, und dass es deswegen dem Anspruch nicht entgegenstehe, wenn mit ihm ein anderer Zweck – hier derjenige der Geltendmachung von Schadensersatzansprüchen – verfolgt werde.

Dies entspricht auch unserer Aufsichtspraxis, nach der für ein Verlangen nach Art. 15 DS-GVO überhaupt keine Begründung erforderlich ist.

Eine weitere Frage, mit der sich der EuGH in der oben genannten Entscheidung befasst hat, betrifft ein Spezifikum im Arzt-Patienten-Verhältnis. Und zwar gibt es im nationalen Recht, genauer gesagt in § 630g des Bürgerlichen Gesetzbuchs (BGB), die Regelung, dass die Patientin und der Patient elektronische Abschriften von der Patientenakte verlangen kann. Gemäß dieser Vorschrift haben sie dem Behandelnden allerdings die entstandenen Kosten zu erstatten. Diese Vorschrift „beißt" sich nun mit der Regelung in Art. 15 Abs. 3 DS-GVO (in Verbindung mit Art. 12 Abs. 5 DS-GVO), nach der die Auskunft verlangende Person unentgeltlich eine erste Kopie verlangen kann. Die Regelung des § 630g BGB wurde bereits vor dem Inkrafttreten der DS-GVO erlassen und dient hinsichtlich des Kostenersatzes dem Schutz der wirtschaftlichen Interessen des für die Verarbeitung Verantwortlichen. Der EuGH hat nun festgestellt, dass es unschädlich sei, dass die nationale Regelung vor dem Inkrafttreten der DS-GVO erlassen worden sei. In Bezug auf den Umstand, dass die Vorschrift hinsichtlich der Regelung zur Kostenerstattung den wirtschaftlichen Interessen des Verantwortlichen dient, ist der EuGH allerdings der Auffassung, dass das Ziel, die wirtschaftlichen Interessen des Behandelnden zu schützen, nicht geeignet sei, um Art. 15 DS-GVO wirksam zu beschränken. In diesem Zusammenhang hat das Gericht hervorgehoben, dass die Datenschutz-Grundverordnung bereits die wirtschaftlichen Interessen der Verantwortlichen mitberücksichtigt habe, in dem z. B. nur die erste Kopie kostenfrei sei. Hieraus schließt der EuGH, dass die Kostenpflicht des § 630g BGB nicht dazu führe, dass der nach Art. 15 DS-GVO Auskunft Verlangende die Auskunft nicht kostenfrei erhält.

Auch dies entspricht der schon vor Erlass des Urteils bestehenden Aufsichtspraxis unserer Behörde, nachdem auch im Arzt-Patienten-Verhältnis der nach Art. 15 DS-GVO Auskunft Verlangende die erste Kopie kostenfrei erhält.

Eine weitere Besonderheit im Arztin-Patienten Verhältnis ergibt sich aus bestimmten satzungsrechtlichen Regelungen der Heilberufskammern (im einschlägigen baden-württembergischen Gesetz als „Heilberufe-Kammern" bezeichnet), die eine Kostenerstattung für die Überlassung von Kopien vorsehen.

Die Berufsordnung der Landesärztekammer Baden-Württemberg enthält in ihrem § 10 Abs. 2 diesen Text:

» *Ärztinnen und Ärzte haben Patientinnen und Patienten auf deren Verlangen unverzüglich in die sie betreffende Patientenakten Einsicht zu gewähren; soweit der Einsichtnahme nicht erhebliche therapeutische Gründe oder erhebliche Rechte der Ärztinnen und Ärzte oder Dritter entgegenstehen. Auf Verlangen sind*

Patientinnen und Patienten Kopien der Unterlagen gegen Erstattung der Kosten herauszugeben. «

Insbesondere auch mit Blick auf solche und vergleichbare satzungsrechtliche Regelungen hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 11. September 2024 die Entschließung „Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern" gefasst.

Wir haben uns entsprechend u. a. an die Landesärztekammer Baden-Württemberg gewandt. Diese Kammer erklärte uns u. a., dass sie sich der Notwendigkeit einer Änderung ihrer Berufsordnung bereits bewusst sei, die Umsetzung allerdings aufgrund bestimmter Umstände noch etwas Zeit in Anspruch nehmen werde und ein Anschreiben unserer Behörde insofern förderlich sein könnte. Wir haben dieser Kammer ein solches Schreiben gesandt und sie gebeten uns mitzuteilen, zu welchem Zeitpunkt sie eine Änderung ihrer Berufsordnung vorsieht, sowie ihre Kammermitglieder in der Übergangszeit bis zur Änderung über die oben genannte Entscheidung des EuGH zum Anspruch auf eine kostenlose Erstkopie der Patientenakte zu informieren und zu einem rechtskonformen Vorgehen anzuhalten.

Die Landespsychotherapeutenkammer Baden-Württemberg, deren Berufsordnung die Vorgaben des EuGH bisher nicht abbildet, hat uns gegenüber erklärt, das Verfahren zur Satzungsänderung werde voraussichtlich im März 2025 beginnen. Die Landeszahnärztekammer Baden-Württemberg hat ihre Berufsordnung bereits angepasst. Im Bereich der Heilberufe ist gemäß Art. 15 DS-GVO auch dann den Patient_innen eine erste Kopie ihrer Behandlungsakten kostenlos zur Verfügung zu stellen, wenn das nationale Recht (etwa § 630g BGB) oder das Berufsrecht einen Anspruch auf Aktenkopie nur gegen Kostenerstattung vorsieht. Das nationale Recht einschließlich des Satzungsrechts der Heilberufskammern sollte insoweit an die europarechtliche Bestimmung in Art. 15 Abs. 3 DS-GVO angepasst werden.

☛ Weiterführende Informationen

Entschließung der DSK „Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden!":
datenschutzkonferenz-online.de/media/en/2024-09-11_Entschliessung_DSK_Patientenakte.pdf

Berufsordnung der Landesärztekammer Baden-Württemberg:
files.aerztekammer-bw.de/c73ea88bf1eb2331/fbaf22825106/Berufsordnung.pdf

Datenschutzrechtliche Prüfung von Webseiten öffentlicher Schulen

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

Im Rahmen des Projekts „Schule digital" (s. S. 113) haben wir für die Schulen eine Fortbildung zum Thema Webseiten an Schulen angeboten. Inwieweit Webseiten an den Schulen datenschutzrechtliche Mängel aufweisen, wollten wir aber auch durch eine Stichprobe herausfinden. Ab dem dritten Quartal 2024 haben wir deswegen Kontrollen in Form einer datenschutzrechtlichen Prüfung von Webseiten öffentlicher Schulen durchgeführt und dabei zahlreiche Mängel und Verbesserungsbedarf festgestellt.

Die meisten öffentlichen Schulen, wenn nicht sogar praktisch alle, betreiben einen Internetauftritt. Für die dabei erfolgende Verarbeitung personenbezogener Daten sind die Schulen, vertreten durch die jeweiligen Schulleitungen, gemäß Art. 4 Nummer 7 DS-GVO verantwortlich.

Dabei kann das Betreiben einer Webseite durch eine öffentliche Schule der Erfüllung ihrer Aufgabe dienen (vgl. zur allgemeinen Aufgabe der Öffentlichkeitsarbeit der vollziehenden Gewalt etwa BVerfG, Urteil vom 27. Februar 2018 – 2 BvE 1 / 16 – Rn. 51) und insoweit die damit verbundene Verarbeitung personenbezogener Daten ggf. ihre Rechtsgrundlage in Art. 6 Abs. 1 Buchst. e) DS-GVO finden. Nicht zuletzt mit Blick darauf, dass solche Webseiten bestimmungsgemäß auch häufig von Schülerinnen und Schülern – und damit typischerweise von Min-

Der LfDI rät dazu, seine FAQ zu Cookies und Tracking zu lesen.

derjährigen – besucht werden, muss die Schule beim Umgang mit den dabei verarbeiteten personenbezogenen Daten die gebotene Sorgfalt anwenden.

Die insgesamt 24 geprüften Schulen wurden von uns über den Schulfinder (schulfinder.kultus-bw.de) so ausgesucht, dass sich eine weitgehend gleichmäßige räumliche Verteilung über die vier Regierungspräsidien und die 21 Schulämter ergab.

Es wurden folgende Aspekte geprüft:

- Einwilligungsbanner (Erforderlichkeit, Anforderungen an eine informierte Einwilligung, täuschende Designpraktiken);
- Implementierung von Drittanbietern (Einwilligungen, korrekte Beschreibung in den Datenschutzinformationen);
- Anforderungen an die Informationssicherheit hinsichtlich https-Verschlüsselung und die Content Security Policy;
- Form und Inhalt der Datenschutzinformationen;
- Veröffentlichung von personenbezogenen Daten auf den Webseiten.

Unsere Prüfung orientierten wir dabei an unseren FAQ Cookies und Tracking.

Einwilligungs-Banner und Implementierung von Drittanbietern

Etwa die Hälfte der geprüften Schulwebseiten wiesen Einwilligungsbanner auf. Einige davon waren überflüssig, da gar keine einwilligungsbedürftige Datenverarbeitung stattfand. Andere waren an verschiedenen Stellen problematisch etwa:

- Fehlen einer Auswahlmöglichkeit (nur Hinweis auf Cookies bei Nutzung der Webseite mit einem „OK" Button);
- Verwendung von täuschenden Designpraktiken (Deceptive Design), etwa durch Hervorheben der Wahlmöglichkeit „Alles akzeptieren" oder erneutes Nachfragen nach Ablehnung;
- Verdecken der Datenschutzinformation durch den Banner, so dass die Information ohne eine vorherige Auswahl nicht zur Kenntnis genommen werden konnte;
- Angabe falscher Rechtsgrundlagen und Angabe von Zwecken, die mit den Aufgaben einer öffentlichen Schule nicht vereinbar sind;
- unzureichende Informationen für eine informierte Einwilligung;
- Auswahlmöglichkeit von Trackingmechanismen.

Grundsätzlich sollten Schulen und andere öffentliche Einrichtungen keine „Cookie-Banner“ oder Einwilligungsbanner haben und keine Daten an Dritte übermitteln, also zum Beispiel keine Analysedienste von Werbekonzernen oder Social-Media-Elemente in ihre Webseite einbinden. Die Anforderungen für rechtskonforme Einwilligungsbanner sind hoch. Im Schulbereich ist das Einholen von Einwilligungen hierfür problematisch, zum einen, weil ein Über- und Unterordnungsverhältnis zwischen der Schule als öffentlicher Einrichtung und den Nutzerinnen und Nutzern der Webseite die Freiwilligkeit der Einwilligung infrage stellen kann (vgl. Erwägungsgrund 43 zur DS-GVO), zum anderen, weil es sich bei den Nutzenden der Webseite vielfach um – überwiegend minderjährige – Schülerinnen und Schüler handeln und daher ihre Einwilligungsfähigkeit fraglich sein kann. Es stellt sich ferner die Frage, inwieweit dies dem öffentlichen Auftrag der Schule dient.

Wir empfehlen den Schulen auf die Implementierung von Drittanbietern etwa externer Kartendienste, Schriftarten, Kalender, implementierte Videos von Videoplattformen etc. möglichst vollständig zu verzichten. Schulen müssen ansonsten darauf achten, dass diese Dienste keine Daten zu eigenen Zwecken verarbeiten, was in der Praxis kaum überprüft werden kann. Schriftarten sollten lokal eingebunden sein. Zur Lokalisation der Schule bietet sich das Geoportal Baden-Württemberg als datenschutzfreundlicher, staatlicher Kartendienst an (geoportal-bw.de). Bei Anbietern mit Drittlandtransfer muss die Schule darüber hinaus die Voraussetzungen nach Kapitel 5 der DS-GVO prüfen.

Einige Schulen hatten Kontaktformulare implementiert. Hier stellt sich zunächst die Frage, an wen die Daten übermittelt werden. Es müssen entsprechende Auftragsverarbeitungs- oder Unterauftragsverhältnisse gegeben sein. Ferner werden hier oft für Schulen merkwürdig anmutende („Firma“) und dem Prinzip der Datenminimierung widersprechende (z. B. vollständige Adresse als Pflichtfeld) Informationen erhoben. Hinzu kommt, dass bei der Eingabe solcher Daten die https-Verschlüsselung der Webseite erzwungen werden muss, was bei vielen Schulen nicht möglich war.

Erfreulicherweise fanden sich auf den 24 Webseiten keine Social Media Plugins, welche direkt Informationen zu diesen Netzwerken senden.

Informationssicherheit

Mit verschiedenen teilweise einfach nutzbaren Techniken können Webseiten zusätzliche Schutzmaßnahmen einführen, um im Falle von Sicherheitslücken in der Software oder bei Angriffen einen zusätzlichen Schutz bieten zu können. Nahezu alle der geprüften Webseiten wiesen Mängel bei diesen auf bzw. haben diese nicht genutzt.

Die sogenannte „Content Security Policy“ (CSP) ist ein Sicherheitskonzept, um verschiedene Angriffe durch Einschleusen von Code und Daten in Webseiten zu verhindern. Damit kann auch „Cross-Site-Scripting“ verhindert werden, das es wiederum erlauben würde, sensible Daten wie Anmeldeinformationen auszulesen. Die Implementation von CSP war oft unvollständig oder gar nicht vorhanden. Die Schulen wurden gebeten, Anpassungen vorzunehmen. Dies erwies sich fachlich für viele Schulen als schwierig.

Die „HTTP Strict Transport Security“ (HSTS) kann verhindern, dass Webseiten-Besucher auf eine unverschlüsselte und damit manipulierbare Variante einer Webseite umgeleitet werden. Der Browser wird damit angewiesen, bei zukünftigen Aufrufen einer Webseite direkt die verschlüsselte und integritätsgesicherte Variante zu verwenden und sollte bei allen Webseiten zum Standard gehören.

DatenschutzInformationen

In fast allen Fällen waren die Datenschutzinformationen unmittelbar von der Webseite und jeder Unterseite aus abrufbar, was erforderlich ist. Manchmal wurden die Informationen unter „Rechtliches“ oder ähnlich gefasst und waren so nicht unmittelbar auffindbar, was geändert werden sollte. In mehreren Fällen widersprachen sich die Informationen auf dem Einwilligungsbanner mit jenen in den separat abrufbaren Datenschutzinformationen. In zwei Fällen war es nicht möglich, sich ohne eine vorherige Auswahl auf dem Einwilligungsbanner näher über die Datenverarbeitung zu informie-

ren. Nur in einem Fall waren gar keine aussagekräftigen Datenschutzinformationen vorhanden, in einem Fall zwei (ein lückenhafter Vordruck des Anbieters plus eine eigene Implementierung).

Das Kultusministerium Baden-Württemberg hat erfreulicherweise einen Vordruck für Datenschutzinformationen auf Schulwebseiten unter it.kultus-bw.de veröffentlicht. Hierbei ist jedoch für die Schulen zu beachten, dass die Informationen an die tatsächliche Datenverarbeitung durch die Webseite angepasst werden müssen. Insbesondere müssen noch Empfänger personenbezogener Daten ergänzt werden, etwa der Web Hoster. Die Löschfristen für Server-Logdateien müssen für den jeweiligen Anbieter angepasst werden. Soweit Drittanbieter implementiert wurden, müssen diese ebenfalls angegeben werden. Auch sollten unzutreffende Informationen zur besseren Lesbarkeit (siehe Art. 12 Abs. 1 DS-GVO) weggelassen werden, etwa zu Cookies, falls die Webseite gar keine Cookies setzt.

Veröffentlichung von personenbezogenen Daten

Hinsichtlich der Veröffentlichung personenbezogener Daten auf den Webseiten wurden die Schulen darauf aufmerksam gemacht, dass dies – mit Ausnahme der Namen und Kontaktdaten der Schulleitung – jeweils einer Einwilligung bedarf, auch von den Lehrkräften. Die Einwilligungserklärungen wurden nicht weiter geprüft.

Erfreulicherweise veröffentlichte keine einzige der geprüften Schulen einen Vertretungsplan auf ihrer Webseite ohne gesonderten Zugang (Intranet der Schule oder zu einem externen Anbieter). Die Veröffentlichung von Vertretungsplänen im Internet hat das Kultusministerium in den FAQ Datenschutz an öffentlichen Schulen (unter: it.kultus-bw.de → Datenschutz an Schulen / Service und FAQ) in begrüßenswerter Weise deutlich ausgeschlossen.

Zusammenfassend ist festzustellen, dass keine einzige der geprüften Schulen die Anforderungen vollumfänglich erfüllt hat.

Viele Schulen meldeten aufgrund unserer Schreiben zurück, dass sie weder die finanziellen Mittel noch die fachliche Expertise besäßen, die Beanstandungen vollumfänglich zu beseitigen bzw. überhaupt die Webseiten unter Beachtung aller relevanten Regelungen zu betreiben (beispielhaft: Datenschutz, Urheberrecht, Barrierefreiheit u.v.m.).

Sofern das Betreiben einer Webseite durch eine Schule im Jahre 2024 erforderlich für die Öffentlichkeitsarbeit der Schule ist, brauchen die Verantwortlichen Unterstützung. Wir können hier nur insofern Hilfestellung leisten, als wir auf datenschutzrechtliche Problemfelder hinweisen und zu deren Vermeidung bzw. hinsichtlich der Beseitigung von Datenschutzmängel beraten können. Es zeigt sich, dass unsere im Rahmen des Projekts „Schule digital" entwickelte Fortbildung zum Thema „Webseiten an Schulen" hierzu wichtige Impulse geben konnte. Angesichts der Prüfungsergebnisse wäre es jedoch wünschenswert, wenn Schulen für diese Aufgabe auch von anderen Stellen Unterstützung erhielten.

☛ Weitere Informationen

FAQ Cookies und Tracking:
www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2

© Illustration: Y. Dwiputri

Abteilung 4: Datenschutz in der Privatwirtschaft

Neues aus dem Bereich Internationaler Datentransfer

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

Homeoffice in Drittstaaten

Wie schon in den Vorjahren erreichten uns auch im Berichtszeitraum mehrere Anfragen zur Zulässigkeit von Homeoffice in Drittstaaten außerhalb der EU aus datenschutzrechtlicher Sicht.

Bereits Anfang des Jahres 2023 hat sich der Europäische Datenschutzausschuss (EDSA) auf einen neuen Transferbegriff geeinigt. Ein Transfer im Sinn von Kapitel 5 der DS-GVO setzt danach dreierlei voraus:

1. Eine verantwortliche oder auftragsverarbeitende Stelle (Exporteur) unterliegt für die betreffende Verarbeitung der DS-GVO. Mit dieser Anforderung werden Direktübermittlungen durch Betroffene in Bezug auf ihre eigenen Daten vom Anwendungsbereich des Kapitels 5 der DS-GVO ausgeschlossen. Zudem folgt daraus, dass Exporteure auch Stellen in einem Drittland gem. Art. 3 Abs. 2 DS-GVO sein können.

2. Der Exporteur legt personenbezogene Daten gegenüber einer anderen verantwortlichen Stelle, einer gemeinsam verantwortlichen Stelle oder einer auftragsverarbeitenden Stelle (Importeur) offen. Beispiele für eine Offenlegung sind das Einrichten eines Accounts, die Gewährung von Zugriffsrechten auf einen bestehenden Account, das Einbinden eines Laufwerks oder das Mitteilen eines Passwortes für eine Datei. Internetveröffentlichungen, die einen freien Abruf durch jedermann ermöglichen, sind damit genauso wenig erfasst wie Datenbewegungen innerhalb eines Verantwortlichen oder Auftragsverarbeiters.

3. Der Importeur befindet sich in einem Drittland, unabhängig davon, ob die DS-GVO gem. Art. 3 Abs. 2 DS-GVO auf ihn anwendbar ist oder nicht.

Anders als bisher gelten nach dieser Definition für Datenbewegungen innerhalb einer verantwortlichen oder auftragsverarbeitenden Stelle (und damit in aller Regel innerhalb einer juristischen Person und eines Unternehmens) – wie etwa beim Transfer zwischen einem Unternehmen in der EU und einer rechtlichen unselbstständigen Filiale außerhalb der EU oder Mitarbeitenden, die sich auf einer Dienstreise oder im Homeoffice in einem Drittstaat aufhalten – die Vorgaben des Kapitels 5 der DS-GVO nicht mehr unmittelbar.

Das bedeutet allerdings nicht, dass die durch das Verbringen der Daten in den Drittstaat geschaffenen besonderen Gefahren bei der datenschutzrechtlichen Betrachtung außen vor bleiben können. Wie der EDSA in seiner Handreichung betont, muss diesen Gefahren im Rahmen von Art. 24 und 32 DS-GVO durch angemessene technische und organisatorische Maßnahmen, die der Exporteur – ggf. unter Mithilfe des Datenimporteurs – festzulegen hat, Rechnung getragen werden. Im Ergebnis ist damit auch in solchen Fällen eine Untersuchung der Rechtslage im Empfängerland (sog. transfer impact assessment, TIA) erforderlich, wie sie im Rahmen von Kapitel 5 der DS-GVO anzustellen wäre. Für Indien, Russland, China, Brasilien, Mexiko und die Türkei hat der EDSA Gutachten zu staatlichen Zugriffen auf personenbezogene Daten veröffentlicht, die in diesem Zusammenhang hilfreich sein können.

Ergeben sich im Einzelfall Risiken durch unverhältnismäßige Zugriffsrechte öffentlicher Stellen des Drittstaats oder durch unzureichenden Rechtsschutz für Betroffene, müssen diese Risiken soweit möglich begrenzt werden; hierfür bieten sich insbesondere die in den Empfehlungen 01 / 2020 des

EDSA aufgeführten ergänzenden Maßnahmen an. Es sind dies:

- Datenspeicherung zu Backup- und anderen Zwecken, die nicht den Zugang zu unverschlüsselten Daten erfordern;
- Übermittlung pseudonymisierter Daten;
- Verschlüsselung von Daten zum Schutz vor dem Zugriff durch Behörden des Drittlands des Datenimporteurs, wenn sich die Daten im Transit zwischen Datenexporteur und Datenimporteur befinden;
- geschützter Empfänger;
- aufgeteilte Verarbeitung oder Verarbeitung durch mehrere Beteiligte (Multi-party Processing).

Überprüfungspflicht hinsichtlich Vorgaben zum Drittstaatentransfer bei auftragsverarbeitenden Stellen

Auf Initiative der dänischen Datenschutzaufsichtsbehörde hat sich der Europäische Datenschutzausschuss (EDSA) in einer im Oktober 2024 veröffentlichten Leitlinie zur Reichweite der Rechenschafts- und Dokumentationspflicht des Verantwortlichen in der Verarbeitungskette geäußert und dabei auch zu der Frage Stellung genommen, inwieweit eine verantwortliche Stelle in der EU selbst überprüfen muss, ob die Vorgaben von Kapitel 5 der DS-GVO bei einem (Onward-)Transfer personenbezogener Daten durch eine (unter-)auftragsverarbeitende Stelle in einen Drittstaat eingehalten werden.

Der EDSA weist zunächst darauf hin, dass einer verantwortlichen Stelle jederzeit – und unabhängig von den mit der Datenverarbeitung verbundenen Risiken – Informationen zur Identität aller in der Verarbeitungskette eingesetzten auftrags- und unterauftragsverarbeitenden Stellen vorliegen müssen (z. B. Name, Adresse und Kontaktperson). Die verantwortliche Stelle benötigt diese Informationen schon allein deshalb, um ihren Pflichten zur Information und Transparenz (Art 13 Abs. 1 Buchst. f), Art. 15 Abs. 1 Buchst. c) DS-GVO) sowie zur Führung eines Verarbeitungsverzeichnisses (Art. 30 Abs. 1 Buchst. d) und e) DS-GVO) vollständig nachkommen zu können.

Auch wenn ein Transfer in einen Drittstaat nicht durch eine verantwortliche Stelle, sondern durch eine von ihm beauftragte auftragsverarbeitende Stelle erfolgt, bleibt die verantwortliche Stelle Adressatin der Pflichten aus Kapitel 5 der DS-GVO. Daraus folgt, dass die auftragsverarbeitende Stelle der verantwortlichen Stelle aussagekräftige Informationen zum Einsatz des gewählten Transferinstrumentes zur Verfügung stellen muss, insbesondere das Transfer Impact Assessment im Fall eines auf die Instrumente des Art. 46 gestützten Transfers. Es ist dann Sache der verantwortlichen Stelle zu entscheiden, ob sie sich auf die Bewertungen der auftragsverarbeitenden Stelle verlässt oder diese hinterfragt und ggf. ergänzende Informationen anfordert. Letzteres ist zumindest dann erforderlich, wenn sich für die verantwortliche Stelle Anhaltspunkte dafür ergeben, dass die von der auftragsverarbeitenden Stelle vorgelegten Unterlagen unvollständig oder unzutreffend sind. Die skizzierte Informationspflicht und Prüfungsobliegenheit gilt für sämtliche in der Verarbeitungskette von (unter-) auftragsverarbeitenden Stellen vorgenommenen Drittstaatenübermittlungen.

Verantwortliche, die auftragsverarbeitende Stellen in einem Drittstaatenkontext einsetzen, sind nach alledem gut beraten:

- die Auftragsdatenvereinbarung(en) daraufhin zu überprüfen, ob darin ausreichende Informationspflichten der auftragsverarbeitenden Stelle gegenüber der verantwortlichen Stelle – auch in Bezug auf etwaige (Weiter-)Übermittlungen in Drittstaaten durch unterauftragsverarbeitende Stellen – vorgesehen sind;
- zu prüfen, ob die auftragsverarbeitende Stelle ihren Informationspflichten auch tatsächlich nachkommt;
- die überlassenen Informationen zu einem Drittstaatentransfer auf Vollständigkeit und Schlüssigkeit hin zu überprüfen.

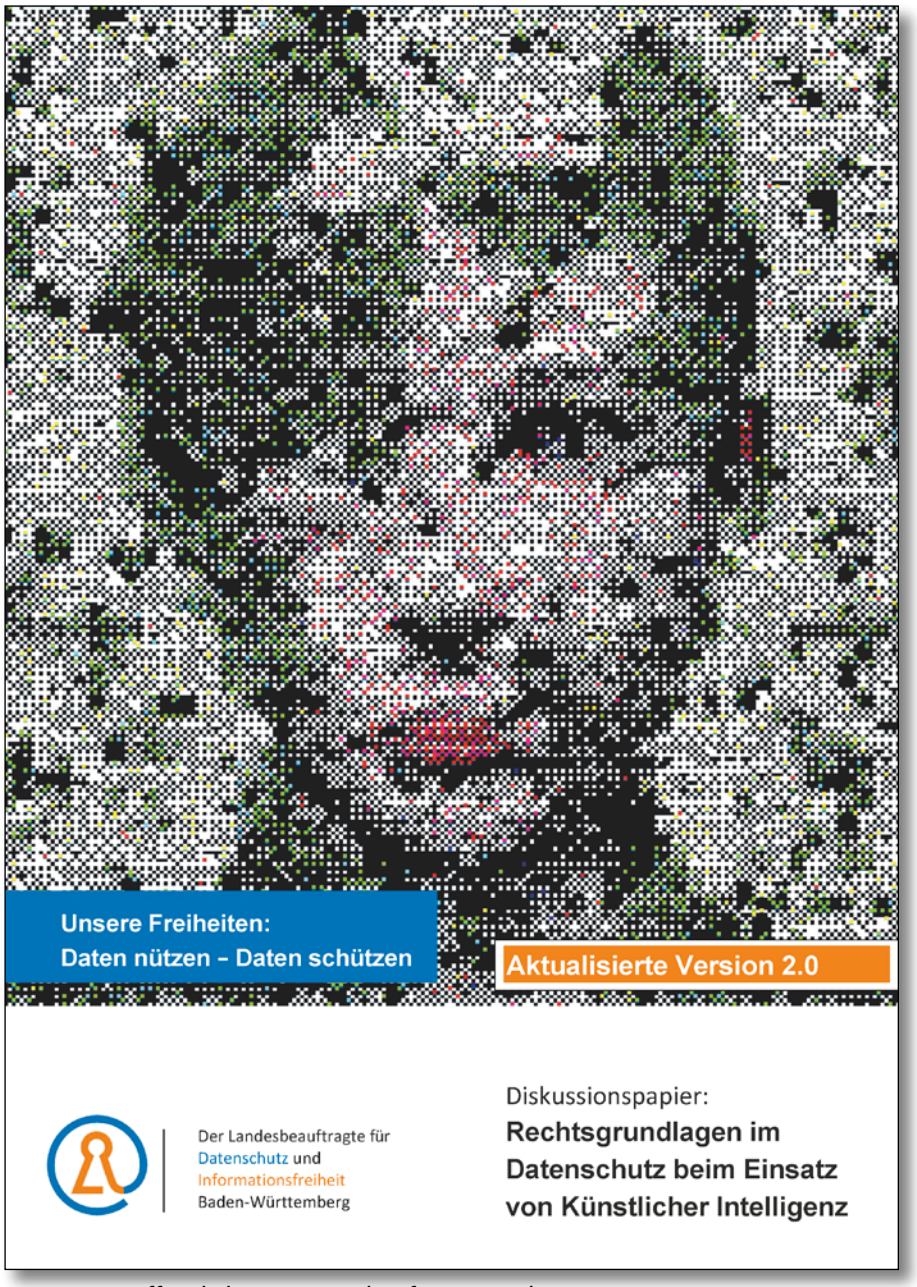
Diskussionspapier 2.0 – Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz

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

Wie oben bereits erwähnt haben wir als erste deutsche Aufsichtsbehörde die „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelli-

genz“ (Version 1.0) vom 7. November 2023 zur öffentlichen Diskussion gestellt (s. auch S. 9 ff.). Seit der Veröffentlichung unseres Diskussionspapiers haben wir zahlreiche Rückmeldungen von Praktiker_innen sowie von Bürger_innen erhalten, die sich an der Diskussion beteiligt haben. Diese Anregungen und Kommentare haben uns wertvolle Hinweise geliefert, die in die Version 2.0 des Papiers eingeflossen sind.

Bei der Überarbeitung des Diskussionspapiers haben wir uns bewusst auf ausgewählte Aspekte konzentriert, die aus unserer Sicht von besonderer Bedeutung sind. Hervorzuheben ist hierbei beispielsweise, dass wir bei der Darstellung der Rechtsgrundlagen eine stärkere Differenzierung zwischen den einzelnen Verarbeitungsphasen vorgenommen haben, sofern sich aus unserer Sicht im Zusammenhang gewisse Besonderheiten ergeben. Darüber hinaus haben wir besonderen Fokus auf die umfangreiche Überarbeitung von Art. 6 Abs. 1 Satz 1 Buchst. f) DS-GVO gelegt, da dieser Rechtsgrundlage in der Praxis eine besondere Bedeutung zukommt. In Anbetracht des offenen Tatbestands von Art. 6 Abs. 1 Satz 1 Buchst. f) DS-GVO und der damit einhergehenden Unsicherheit in der Anwendung haben wir für zwei aktuelle Praxisbeispiele wesentliche KI-spezifische Aspekte einer Interessenabwägung herausgearbeitet.



Bildmotiv: local_doctor – stock.adobe.com

Seit Erstveröffentlichung ein viel gefragtes Diskussionspapier.

Wir haben die Überarbeitung unseres Papiers aber auch zum Anlass genommen, weitere datenschutzrelevante Bereiche einzuarbeiten bzw. auszubauen. Ein besonderes Augenmerk lag dabei auf dem Datenschutz in Schulen, da dieser in Zeiten der Digitalisierung mit der Nutzung digitaler Tools und von KI im Unterricht (z. B. Lernplattformen mit adaptiven Elementen) eine immer größere Bedeutung gewinnt. Die Nutzung solcher innovativer Systeme im schulischen Kontext ist allerdings regelmäßig besonders eingriffsintensiv, und die Verarbeitung personenbezogener Daten Minderjähriger steht unter einem besonderen Schutz der DS-GVO (vgl. Art. 8 DS-GVO). Aus diesem Grund haben wir das Diskussionspapier um einen weiteren Abschnitt ergänzt, der sich mit den Rechtsgrundlagen für den Einsatz von KI-Anwen-

dungen in Schulen beschäftigt und einige Spezifika aufzeigt. Aufgrund der besonderen Praxisrelevanz haben wir überdies auch die Thematik des Personenbezugs von KI-Systemen weiter ausgebaut.

Insgesamt wird es im Zuge der stetig voranschreitenden Digitalisierung auch zukünftig unsere Aufgabe sein, regelmäßige Überprüfungen und Anpassungen vorzunehmen, um den datenschutzrechtlichen Herausforderungen neuer Technologien gerecht zu werden. Dies ist notwendig, um eine Balance zwischen technologischem Fortschritt und dem notwendigen Schutz personenbezogener Daten aufrechtzuerhalten. Das Diskussionspapier: Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz, Version 2.0 vom 17. Oktober 2024 wird insoweit auch weiterhin ein „lebendes" Dokument bleiben.

Weitere Informationen

Orientierungshilfen-Navigator KI & Datenschutz – ONKIDA:
www.baden-wuerttemberg.datenschutz.de/onkida

Diskussionspapier Rechtsgrundlagen beim Datenschutz beim Einsatz von Lünstlicher Intelligenz, Version 2.0:
www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

Beratung Start-Ups und KMU – Datenschutz von Anfang an mitgedacht!

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

In den vergangenen Jahren haben die Anforderungen des Datenschutzes an Unternehmen zugenommen, was nicht zuletzt auch an der fortlaufenden Digitalisierung liegt. Bei der Verarbeitung personenbezogener Daten gilt die DS-GVO für Vereine und kleine Betriebe genauso wie für große Konzerne – und für Start-Ups. Während große Unternehmen oftmals über eigene (externe) Datenschutzbeauftragte oder eigene Rechtsabteilungen verfügen, stehen Start-Ups sowie kleine und mittlere Unternehmen (KMU) regelmäßig vor der Herausforderung, die umfangreichen Anforderungen der DS-GVO eigenständig und möglichst kostengünstig umzusetzen. Dabei ist es besonders wichtig, dass gerade in der Gründungsphase eines jungen Unternehmens der Datenschutz bereits von Anfang an mitgedacht wird. Um diesen steigenden Bedarf zu decken, haben wir, wie bereits im 39. Tätigkeitsbericht Datenschutz angekündigt (vgl. S. 31 ff.), unser Beratungs- und Schulungsangebot für junge Unternehmen sowie die Zusammenarbeit mit den Digitalisierungsakteuren aus Baden-Württemberg, etwa dem Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg, auch im vergangenen Jahr weiter ausgebaut.

Zu Beginn richtete sich das Angebot unserer Behörde vor allem an Start-Up-Unternehmen. Im vergangenen Jahr haben wir das Beratungsangebot – an das entsprechende Angebot vor Geltung der DS-GVO anknüpfend – auf KMU ausgeweitet, da wir auch in diesem Bereich weiterhin einen großen Beratungsbedarf im Datenschutzbereich festgestellt haben. Gerade kleinere Unternehmen, die häufig auf externe Beratung angewiesen sind, sollen von unserer Expertise und unserem Angebot profitieren. Wir bieten mithin eine allgemeine datenschutzrechtliche Beratung an, die individuell auf die Bedürfnisse der jeweiligen Unternehmen zugeschnitten ist. Unternehmen aus Baden-Württemberg können dabei in Bezug auf ihre konkreten Fragestellungen, etwa den Umgang mit Kundendaten, die rechtliche Ausgestaltung von Geschäftsprozessen im Einklang mit der DS-GVO oder die Implementierung von Löschkonzeptionen, unsere Unterstützung einholen. Da eine solche intensive Beratung unter Ressourcenvorbehalt steht, haben wir zudem die Schulungsreihe „Basiswissen im Datenschutz für Klein(st)unternehmen, Selbstständige und Start-Ups" ins Leben gerufen und damit zusätzlich eine spezielle Schulung für unser hauseigenes Bildungszentrum (BIDIB) erstellt, die über die allgemeine Beratung hinausgeht und sich tiefergehend mit den grundlegenden Themen des Datenschutzes auseinandersetzt und zugleich jungen Unternehmer_innen praxisnahe Lösungsmöglichkeiten aufzeigt. Wir haben dabei gezielt einen Schwerpunkt auf datenschutzrechtliche Themen gelegt, die im Unternehmensalltag

Der LfDI berät Jungunternehmerinnen und -unternehmer.

von kleinen Unternehmen eine besondere Rolle spielen. Über diese systemische Beratung wollen wir möglichst viele Unternehmen erreichen.

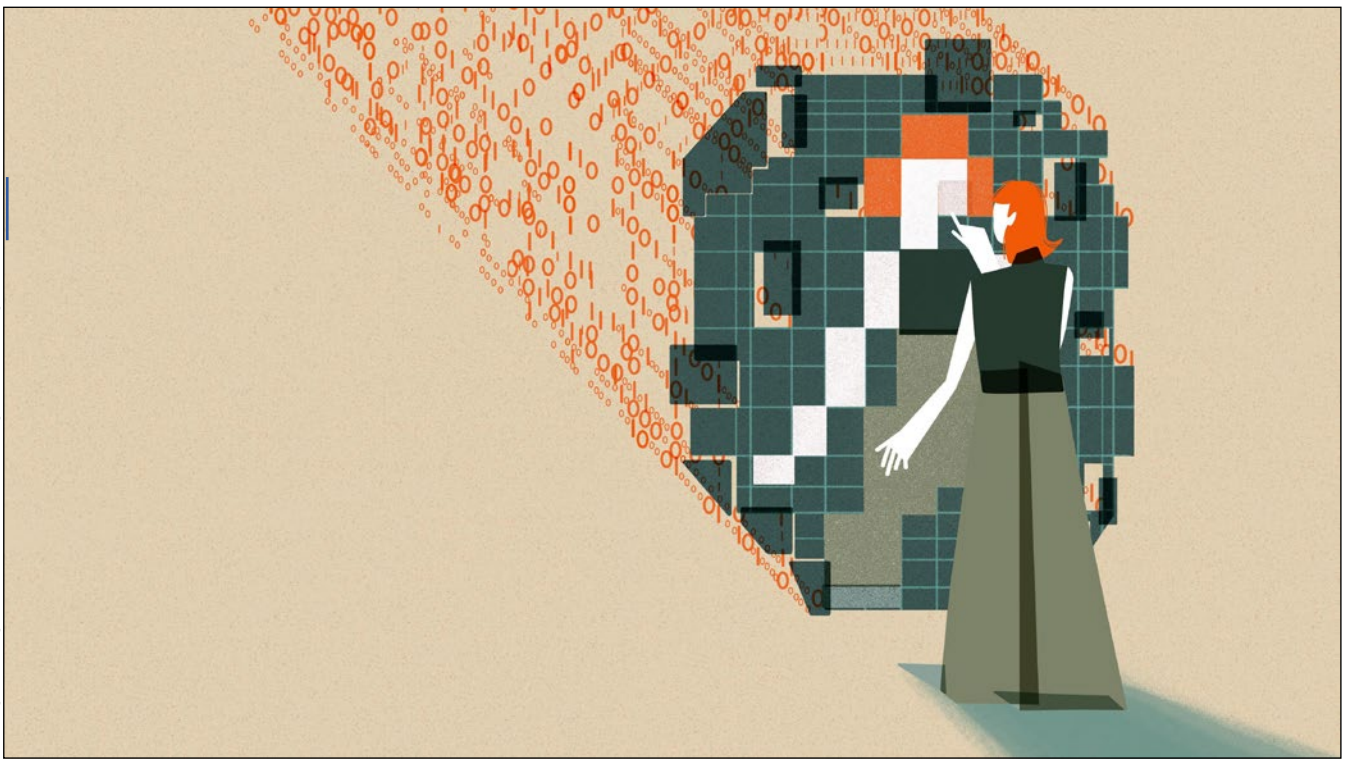
Einen weiteren Schwerpunkt haben wir zudem in diesem Jahr wieder auf den aktiven Austausch mit Akteuren der Digitalisierung gelegt. In diesem Zusammenhang haben wir unter anderem an verschiedenen Veranstaltungen der Start-Up-Szene teilgenommen (z. B. dem Start-up BW Summit 2024). Dabei stand der Dialog mit jungen Unternehmer_innen und Innovator_innen im Vordergrund, um gemeinsam Herausforderungen und Chancen im Datenschutz zu erörtern. Diese Veranstaltungen boten für uns eine wertvolle Gelegenheit, die Bedürfnisse der Praxis zu verstehen und gezielt auf deren Anforderungen einzugehen. Unser Ziel ist es dabei, sicherzustellen, dass Datenschutz in der dynamischen Start-Up-Szene als integraler Bestandteil verstanden wird.

Auch in Zukunft wollen wir unsere Kooperationen im Land weiter ausbauen und als Ansprechpartner rund um Digitalisierungsthemen verstanden werden. Insoweit wäre auch eine Zusammenarbeit mit dem IPAI Heilbronn zielführend, um eine effektive und nachhaltige Entwicklung innovativer Technologien – insbesondere in kleineren Unternehmen – zu unterstützen. Eine möglichst frühe Einbindung der Datenschutzaufsicht in Digitalisierungsprojekte und damit ein von Anfang an mitgedachter Datenschutz bedeutet zugleich mehr Wirtschaftlichkeit und Skalierbarkeit der Projekte und fördert darüber hinaus eine erfolgreiche und rechtssichere Innovationsentwicklung in Baden-Württemberg.

☛ Weitere Informationen

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

Bildungszentrum BIDIB: www.baden-wuerttemberg.datenschutz.de/bildungszentrum



KI kann sehr nützlich sein, aber auch ein Haftungsrisiko darstellen.

Einsatz von KI-Tools in der Praxis

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

KI-Anwendungen können sehr nützlich sein, aber zugleich auch ein Haftungsrisiko darstellen, wenn Verantwortliche sich nicht frühzeitig mit den rechtlichen Anforderungen beschäftigen. Wir zeigen am Beispiel eines KI-Tools zur Transkription, was beim Einsatz aus datenschutzrechtlicher Sicht zu beachten ist.

Uns erreichte eine Beratungsanfrage zu einem KI-Tool, das speziell für die Transkription von Online-Veranstaltungen und virtuellen Besprechungen eingesetzt werden soll. Mit Hilfe des Tools sollen gesprochene Inhalte in Echtzeit aufgezeichnet und automatisch in das geschriebene Wort umgewandelt werden, was eine händische Protokollierung der Veranstaltung überflüssig machen und damit eine Nachbereitung vereinfachen soll. Im Regelfall werden dabei jedoch gleichermaßen personenbezogene Daten wie beispielsweise Nutzendeninformationen oder das gesprochene Wort von Teilnehmenden verarbeitet. Der Einsatz eines solchen KI-Tools wirft mithin datenschutzrechtliche Fragen auf, die sorgfältig geprüft werden müssen. Die Einhaltung der Datenschutz-Grundverordnung (DS-GVO) ist damit unerlässlich.

Bei der Bearbeitung der Anfrage haben wir insoweit zuerst geprüft, welche Parteien aktiv an der Datenverarbeitung beteiligt sein könnten und wie die datenschutzrechtliche Rollenverteilung ausgestaltet ist. Dies ist wichtig, da die verantwortliche Stelle i. S. v. Art. 4 Nummer 7 DS-GVO die Verantwortung für die Verarbeitung personenbezogener Daten trägt, vgl. Art. 5 Abs. 1, Art. 24 Abs. 1 Satz 1 DS-GVO. Allgemein kann dabei festgehalten werden, dass mit der Entscheidung, ein KI-Tool im Rahmen einer Online-Veranstaltung zu nutzen, grundsätzlich die Verantwortlichkeit im Sinne des Art. 4 Nummer 7 DS-GVO einhergeht. Wer die KI anbietet, wird in diesem Zusammenhang regelmäßig auch die Rolle der Auftragsverarbeitung einnehmen, so dass ein Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO abgeschlossen werden muss. Die verantwortliche Stelle hat dann zu prüfen, inwieweit die gesetzlichen Vorgaben des Art. 28 DS-GVO eingehalten werden. Solche Vereinbarungen müssen regelmäßig die Nutzung zu

eigenen Zwecken, in diesem Kontext insbesondere zu Trainingszwecken der KI, untersagen bzw. dürfen diese nicht erlauben. Unabhängig hiervon sollte die verantwortliche Stelle allerdings stets eigenständig nachprüfen, ob und inwieweit die KI Anbietenden / KI Entwickelnden nicht doch ggf. auf personenbezogene Daten für eigene Zwecke (z. B. für KI-Trainingszwecke) zugreifen. In diesem Fall wäre er dann grundsätzlich nicht als auftragsverarbeitend anzusehen, da für die Eigenschaft als verantwortliche Stelle ausschließlich der tatsächliche Einfluss maßgebend ist. Dementsprechend sollten ausreichende Vorkehrungen gemäß Art. 25 DS-GVO getroffen werden, um datenschutzrechtsrelevante Zugriffe zu unterbinden. Hierzu kann unter anderem auch gehören, dass die Datenverarbeitung für Zwecke der Anbietenden bzw. Entwickelnden sowohl vertraglich als auch faktisch kontrolliert und unterbunden wird (z. B. Deaktivierung des KI-Trainingsmodus, v. a. bei Drittanbietenden).

Ausgehend von der Verantwortlichkeit muss sichergestellt werden, dass die datenschutzrechtlichen Anforderungen beim Einsatz des KI-Tools umfassend eingehalten werden. Zu nennen sind hier insbesondere die Frage der Rechtsgrundlage sowie die Informationspflichten.

Wir haben die verantwortliche Stelle darauf hingewiesen, dass die Teilnehmenden bereits vor der Datenverarbeitung entsprechend den Maßgaben nach Art. 13 DS-GVO über die Datenverarbeitung – also z. B. den Einsatz des KI-Tools zum Zweck der Aufzeichnung und Transkription – umfassend informiert werden müssen. Eine entsprechende Information sollte den Teilnehmenden daher bereits frühzeitig mit der Einladung zur Online-Veranstaltung übermittelt werden. Zudem kann es empfehlenswert sein, wenn die Teilnehmenden bei der Veranstaltung nochmals vor der Aufzeichnung durch ein Pop-up-Fenster informiert werden, das sie aktiv wegklicken müssen.

Ebenso haben wir die verantwortliche Stelle darauf hingewiesen, dass sie sicherstellen und damit letztlich abschließend prüfen muss, ob die Verarbeitung personenbezogener Daten mit Hilfe eines KI-Tools durch eine einschlägige Rechtsgrundlage gedeckt ist. Diese kann sich grundsätzlich neben spezialgesetzlichen Vorschriften insbesondere aus Art. 6 DS-GVO sowie für die Verarbeitung besonderer Kategorien personenbezogener Daten aus Art. 9 Abs. 2 DS-GVO ergeben. Für den Einsatz eines KI-Tools und die damit zusammenhängende Datenverarbeitung kommt in der Praxis neben der Wahrung berechtigter Interessen nach Art. 6 Abs. 1 Buchst. f) DS-GVO häufig eine Einwilligung nach Art. 6 Abs. 1 Buchst. a) DS-GVO in Betracht. Deren Erklärung sollte dabei unter anderem kenntlich machen, dass es sich um eine Einwilligungserklärung handelt, konkret und leicht verständlich formuliert sein, klar ausdrücken, zu welchem Zweck die Daten verarbeitet werden sollen, und Hinweise zur Speicherdauer der Daten enthalten. Letztlich könnte eine Einwilligung sogar erforderlich sein, insbesondere dann, wenn im Einzelfall auch besonders geschützte Daten nach Art. 9 DS-GVO (wie z. B. Gesundheitsdaten) Gegenstand der Transkription sind und ein Rückgriff auf die Rechtsgrundlage Art. 6 Abs. 1 Buchst. f) DS-GVO nicht mehr in Betracht kommt. Denkbar wäre dies vor allem für den Fall, dass Teilnehmende mitunter sensible Informationen über ihren Gesundheitszustand aktiv preisgeben und diese dann verarbeitet werden.

Bis hierher handelt es sich allein um die datenschutzrechtlichen Anforderungen. Zu beachten gilt überdies, dass in Deutschland das gesprochene Wort besonders geschützt ist. So kann sich nach § 201 StGB strafbar machen, wer das nichtöffentlich gesprochene Wort unbefugt – d. h. ohne Einverständnis – auf einen Tonträger aufnimmt. Vor diesem Hintergrund kann ebenfalls eine (zumindest stillschweigende oder mutmaßliche) Einwilligung erforderlich sein.

Insgesamt zeigt dieser Fall betreffend den Einsatz eines KI-Tools zur Datenverarbeitung anschaulich, dass verantwortliche Stellen sich frühzeitig mit den datenschutzrechtlichen Anforderungen vertraut machen sollten. Wichtig ist dabei, dass bei der Verarbeitung personenbezogener Daten durch KI-Systeme intern klare Richtlinien und Zuständigkeiten im Umgang mit KI-Systemen geschaffen werden. Daneben sollten die Beschäftigten in besonderem Maße sensibilisiert und geschult werden. Auch regelmäßige Datenschutz-Audits und KI-Monito-

rings sollten fester Bestandteil eines funktionsfähigen KI-Datenschutz-Konzepts sein.

Weitere Informationen

Formulierungshilfe für Auftragsverarbeitungsvertrag: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/muster_adv.pdf

Diskussionspapier unter: www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki

ONKIDA (abrufbar unter: www.baden-wuerttemberg.datenschutz.de/beitrag-orientierungshilfen-navigator-ki-datenschutz

Weitere Hilfestellungen zum Einsatz von KI: LDA Bayern: www.lda.bayern.de/de/ki.html

Vereine unterstützen, Wissen zur Verfügung stellen

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

Die gesamtgesellschaftliche Bedeutung des Ehrenamtes ist nicht zu unterschätzen. Dementsprechend sind wir gerade bei Vereinen unterstützend und beratend tätig. So haben wir unsere Expertise im Berichtszeitraum nicht nur in diversen internen und externen Schulungen, sondern auch bei Initiativen von Landtagsabgeordneten zur Unterstützung des Ehrenamtes eingebracht. Sofern wir im Rahmen unserer aufsichtsbehördlichen Tätigkeit datenschutzwidrige Verarbeitungsvorgänge vorfinden, agieren wir primär mit dem Ziel der Abhilfe und nicht der Sanktionierung. Zwei exemplarische Beispiele zeigen, wie sinnvoll es ist, Vereinen zur Seite zu stehen.

Als Vereinsmitglied grenzenlos fotogen?

Die datenschutzrechtliche Zulässigkeit von Fotoaufnahmen gehört sicherlich zu den Dauerbrennern im Datenschutzrecht. Unser entsprechendes Infomaterial erfreut sich größter Beliebtheit. Gleichwohl erreichen uns auch immer wieder Beschwerden von Betroffenen.

Im Rahmen einer Beschwerde gelangte uns eine problematische Beitrittserklärung eines Sportvereins zur Kenntnis: Um nicht lästige Einzeleinwilligungen zu womöglich einzelnen Fotos bei seinen Mitgliedern zeitaufwändig einholen zu müssen, war eine Art Generalerlaubnis bei der Mitgliederaufnahme vorgesehen. Neben den üblichen Angaben zur Person wie Name, Adresse und Beitragsmodalitäten wurde im Mitgliedsantrag hinsichtlich Fotoaufnahmen eine erstaunlich weite Veröffentlichungseinwilligung eingefordert, so dass jedwede Fotoveröffentlichung im Vorfeld durch die Beitrittswilligen abgesegnet werden sollte.

So hieß es dort (sinngemäß): „Ich gebe meine Einwilligung zur Verarbeitung meiner personenbezogenen Bilddaten. Als Verein wollen wir unsere Aktivitäten sowohl auf unserer Homepage als auch in gedruckter Form präsentieren. Dies ist nur mit Ihrem Einverständnis möglich. Einer Veröffentlichung auf der Vereinshomepage (…) stimme ich zu. Hinweis: Bitte haben Sie Verständnis, sollten die Einwilligungen nicht oder nur teilweise erteilt werden, so wird der Verein der Mitgliedschaft nicht zustimmen."

Dieser klassische Fall der Koppelung eines Vereinsbeitritts mit der Einwilligung in sehr unbestimmte Fotoaufnahmen und deren Veröffentlichungen war nach unserer Einschätzung – auch nach entsprechender Anhörung des Vereins – zur Teilnahme am Vereinsleben grundsätzlich nicht erforderlich. Es war für uns insbesondere nicht ersichtlich, dass ohne die Veröffentlichungen der Satzungszweck nicht erfüllt werden könnte. Nach unserer Anfrage wurde das entsprechende Beitrittsformular den Vorgaben der DS-GVO angepasst. Künftig können neue Mitglieder auch dann Aufnahme im Verein finden, wenn sie keine (pauschale) Einwilligung im Hinblick auf die Aufnahme und anschließende Veröffentlichung der Fotos abgeben. Unberührt hiervon bleiben jedoch Fotoveröffentlichungen, die der Verein auf andere rechtliche Grundlagen stützen kann (vgl. die Ausführungen zum „berechtigten Interesse" im Infokasten.)

Eine Pflicht zur Aufnahme von Vereinsmitgliedern im Sinne eines Vertragszwanges besteht selbstverständlich nicht. Wenn der Verein insofern eine Person nicht als Mitglied aufnehmen will, so steht

Für Vereine und kleine Betriebe: Das LfDI Tool DS-GVO.clever.

ihm diese Entscheidung als Ausfluss der Vertragsfreiheit natürlich zu. Soweit er dies jedoch an die fehlende Einwilligung für Foto- oder Videoaufnahmen koppelt, verstößt er grundsätzlich gegen datenschutzrechtliche Vorgaben (zu im Einzelfall zulässigen Koppelungen s. unseren 39. Tätigkeitsbericht Datenschutz 2023, S. 109 f.).

In einer anderen Sache beschwerte sich die Mutter eines Kindes darüber, dass die Übungsleiterin im Schnupperkurs Kinderturnen ohne ihre Zustimmung Fotos von ihrem Kind gemacht und diese in einer WhatsApp-Gruppe versendet hatte, der neben der Übungsleiterin verschiedene Eltern angehörten.

Der Verein stellte sich sowohl gegenüber der Mutter als auch uns gegenüber auf den Standpunkt, dass es sich zum einen um eine Sache der Übungsleiterin handele, zum anderen das betroffene Kind nicht Mitglied sei, weshalb es keine Angelegenheit für den Verein sei. Hierbei handelte es sich offensichtlich um eine Fehleinschätzung durch den Verein, da es sich um ein offizielles Vereinsangebot handelte. Dementsprechend war der Verein datenschutzrechtlich verantwortlich und hatte entsprechende Vorgaben zu beachten. Unabhängig von dem grundsätzlich problematischen Verbreiten von Kinderbildern über WhatsApp bedarf eine solche Verarbeitung der ausdrücklichen Einwilligung der Erziehungsberechtigten. Eine andere Rechtsgrundlage kommt hierfür nicht in Betracht. Da der Verein keine Einwilligung der Mutter bzw. der Eltern nachweisen konnte, haben wir die entsprechende Aufnahme und Verbreitung als datenschutzwidrig beanstandet. Der Verein hat uns zwischenzeitlich dahingehend informiert, dass zukünftig keine Fotos ohne ausdrückliche Einwilligung der betroffenen Personen bzw. der Erziehungsberechtigten aufgenommen und weiterverbreitet werden.

Vereine sollten sich im Vorfeld einer Datenverarbeitung Gedanken zur Rechtsgrundlage machen. Hierbei kann unser Informationsmaterial spätere Beschwerden betroffener Personen verhindern.

☛ Mehr Informationen

Allgemein zu Fotoveröffentlichungen können folgende Informationen unserer Aufsichtsbehörde auf unserer Homepage abgerufen werden:

FAQ Veröffentlichung von Fotos speziell für Vereine:
www.baden-wuerttemberg.datenschutz.de/faq-veroeffentlichung-von-fotos-speziell-fuer-vereine

Die Orientierungshilfe „Datenschutz im Verein nach der DS-GVO“:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf

Der Praxisratgeber für Vereine:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/06/Praxisratgeber-f%C3%BCr-Vereine.pdf

39. Tätigkeitsbericht Datenschutz des LfDI BW:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2024/02/TB_39_DS_barrierefrei.pdf

Den betroffenen Vereinen geben wir regelmäßig folgende Informationen zur Fotoerstellung und -veröffentlichung im Vereinskontext:

Einwilligung: Eine verantwortliche Stelle (Verein) darf personenbezogene Daten nur verarbeiten, wenn ihr dafür eine Rechtsgrundlage zur Verfügung steht. Eine mögliche Rechtsgrundlage zur Verarbeitung personenbezogener Daten kann sich hierbei durchaus aus einer erteilten Einwilligung der betroffenen Person ergeben (vgl. Art. 6 Abs. 1 Satz 1 Buchst. a) DS-GVO). Die Einwilligung ist insbesondere ein Instrument der Selbstbestimmung. Die rechtlichen Voraussetzungen, die an die Art und Weise der Erteilung einer wirksamen Einwilligung zu stellen sind, ergeben sich aus den Art. 7 und 8 DS-GVO. Insbesondere muss die erteilte Einwilligung freiwillig erteilt werden, vgl. Art. 7 Abs. 4 DS-GVO. Eine Einwilligung ist nur dann wirksam erteilt, wenn die betroffene Person ausreichend über die Umstände der Verarbeitung informiert wird, bevor es zur Verarbeitung personenbezogener Daten kommt.

Freiwilligkeit: Es kann z. B. nur dann davon ausgegangen werden, dass eine betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte und freie Wahl hat, also in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (siehe Erwägungsgrund – ErwGr. – 42 der DS-GVO). Dies ist z. B. dann nicht der Fall, wenn die Aufnahme in den Verein von einer Einwilligung in eine Datenverarbeitung – wie z. B. einer Veröffentlichung auf der Homepage – abhängig gemacht wird. Die Begründung hierfür ist, dass die Veröffentlichung der Mitgliederdaten im Internet nicht für die Erfüllung des Vertrages (bzw. die Mitgliedschaft im Verein) erforderlich ist (Art. 7 Abs. 4 i.V.m. ErwGr. 43 DS-GVO).

Satzungszweck / Vertrag: Für die Vereinsaufnahme (Vertragsabschluss) dürfen nur die für einen Vertragsabschluss oder bei dessen Durchführung notwendigen personenbezogenen Daten verarbeitet werden. Soweit ein Verein anlässlich eines Vertragsabschlusses (zur Mitgliedschaft) oder später personenbezogene Daten, die nicht für die Begründung des Vertrages oder für seine Durchführung erforderlich sind, erheben oder verarbeiten möchte, kann dies regelmäßig nur dann erfolgen, wenn die betroffene Person hierzu eine wirksame Einwilligung erteilt hat. Sie ist jedoch nur verbindlich, wenn der betroffenen Person klar ist, dass die Datenverarbeitung mit dem Mitgliedsvertrag nichts zu tun hat und dass die betroffene Person die Freiheit hat, die Zustimmung zu verweigern, ohne den Vertrag (hier: die Vereinsmitgliedschaft) oder dessen Durchführung dadurch zu gefährden.

Berechtigtes Interesse als Rechtsgrundlage (Art. 6 Abs. 1 Satz 1 Buchst. f) DS-GVO): Die Einwilligungserklärung bzw. Teile von ihr sind unbeachtlich, soweit sie gegen die DS-GVO verstoßen oder unter Verstoß gegen zwingende Vorschriften zustande gekommen sind, vgl. Art. 7 Abs. 2 Satz 2 DS-GVO. Insbesondere ist sie unwirksam bei Verstößen gegen den Erforderlichkeitsgrundsatz bzw. das „Kopplungsverbot". Die DS-GVO schließt nicht aus, dass die Datenverarbeitung rechtmäßig erfolgt, wenn zwar die Einwilligung unbeachtlich ist, der Datenverarbeitungsvorgang aber durch eine gesetzliche Vorschrift legitimiert ist. Dies wäre z. B. gegeben, wenn eine Fotoveröffentlichung im überwiegenden berechtigten Interesse des Vereins (vgl. Art. 6 Abs. 1 Satz 1 Buchst. f) DS-GVO) erfolgen darf, z. B. im Hinblick auf die Ablichtung der drei Erstplatzieren für eine Presseveröffentlichung im Rahmen der Ergebnisveröffentlichung bei einem Sportwettkampf. Dann ist die Verarbeitung zur Wahrung der berechtigten Interessen der verantwortlichen Stelle (des Vereins) erforderlich, da die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Jedoch ist auch hier nicht jede beliebige Fotoveröffentlichung gedeckt, denn wenn es z. B. um die Verarbeitung von personenbezogenen Daten von Kindern geht, besteht eine besondere Schutzpflicht, so dass alle speziell hier anfallenden Abwägungselemente zu berücksichtigen sind.

Zur Erforderlichkeit einer Personalausweiskopie zur Plattformnutzung

Betroffene Personen können sich auch mit Hinweisen an uns wenden. Sofern ein Tätigwerden geboten erscheint, gehen wir in solchen Fällen auf die Verantwortlichen zu mit dem Ziel, den mutmaßlichen datenschutzwidrigen Zustand zu beseitigen. Bei der Verwendung von Personalausweisdaten, insbesondere der Erstellung von Kopien, sind strenge Grenzen zu beachten, insbesondere der Grundsatz der Erforderlichkeit.

Nutzende einer Plattform bei einem eingetragenen Verein, der im Sektor Kommunikation im Gesundheitsbereich eines Berufsverbandes tätig ist, hatten zur Registrierung neben der Vorlage einer Kopie des Ausbildungsabschlusses auch die Speicherung und Verarbeitung ihrer Personalausweiskopie zu akzeptieren, um die Leistung des Vereins (Nutzung der Plattform) in Anspruch nehmen zu können. Der Verein begründete dies mit der Notwendigkeit eines geschützten kollegialen Austauschs. Alle Mitglieder sollten die Möglichkeit haben, Informationen ohne unerwünschte Mitleserschaft weitergeben zu können.

Durch einen Hinweise wurden wir hierauf aufmerksam gemacht und wandten uns mit verschiedenen Fragen an den Verein. So war für uns insbesondere nicht erkennbar, auf welcher Rechtsgrundlage die Personalausweisdaten erhoben wurden, wofür die Kopie des Personalausweises neben der Kopie des Ausbildungsabschlusses erforderlich war, wieso sämtliche Personalausweisdaten erhoben wurden und wie lange die entsprechenden Daten gespeichert wurden.

Die Notwendigkeit der Erhebung der Ausweiskopien wurde von dem Verein damit begründet, dass z. B. Mitarbeitende von Krankenkassen Kopien der Ausbildungsabschluss-Urkunden verwenden könnten, um sich für den geschützten Bereich des vom Verein betriebenen Portals anzumelden. Nach einschlägiger Rechtsprechung, z. B. des Bundesverwaltungsgerichts zur Erforderlichkeit einer Videoüberwachung, ist jedoch „(n)ach dem allgemein anerkannten Begriffsverständnis (…) Erforderlichkeit [nur dann] anzunehmen, wenn ein Grund, etwa eine Gefährdungslage, hinreichend durch Tatsachen oder die allgemeine Lebenserfahrung belegt ist, und ihm nicht ebenso gut durch eine andere, gleich wirksame, aber schonendere Maßnahme Rechnung getragen werden kann."

Mit Blick hierauf fragten wir nach, inwieweit es in der Vergangenheit zu entsprechenden missbräuchlichen Verwendungen kam oder woraus sich die notwendige hinreichende Verdachtslage einer solchen missbräuchlichen Verwendung ergab.

Es stellte sich heraus, dass die Personalausweiskopie zur Registrierung vom Verein vorsorglich festgelegt wurde, um missbräuchliche Registrierungen zu verhindern. Der Verein hat das vorliegende Verfahren schließlich zum Anlass genommen, den Registrierungsvorgang, der für unsere Überprüfungsdauer gesperrt war, einer erneuten Überprüfung zu unterziehen. Dabei kam der Verein zu dem Ergebnis, dass zukünftig auf die Anforderung einer Kopie des Personalausweises verzichtet werden soll. Stattdessen würden manuell berufliche E-Mail-Adressen geprüft. In Zweifelsfällen würden Anfragen zur Anmeldung gestellt. Zudem würden keine Personalausweiskopien mehr gespeichert werden.

Unsere datenschutzrechtliche Überprüfung ergab somit, dass die Verarbeitung der Personalausweisdaten der Plattformnutzenden ohne Rechtgrundlage erfolgte. Aufgrund der Anpassungen und Nachbesserungen sowie der entsprechenden Umsetzungsmaßnahmen des Vereins wurde auf weitergehende aufsichtsbehördliche Maßnahmen verzichtet.

Keine Hürden bei der Newsletter-Abmeldung

✎ Art. 57 Abs. 1 Buchst. f) DS-GVO

Mehrere Beschwerden im Berichtszeitraum betrafen das Verfahren bei der Abmeldung vom zuvor abonnierten Werbe-Newsletter. Diesen Beschwerden war gemeinsam, dass die jeweilige verantwortliche Stelle gewisse Hürden in das Abmelde-Ver-

fahren eingebaut hatte, um, so zumindest unsere Einschätzung, das Abmeldeverfahren möglichst zu erschweren.

So wurde in einer Beschwerde gegen einen Lebensmittel-Discounter moniert, dass der Abmeldelink in der Newsletter-Mail zunächst auf eine Internetseite des Unternehmens führte. Dort musste man zunächst die betroffene E-Mail-Adresse eintragen und als Pflichtoption durch das entsprechende Ankreuzen einer Checkbox eine Auswahl treffen, ob man weniger oder gar keinen Newsletter mehr erhalten möchte. Erst dann war eine Abmeldung oder Änderung möglich.

Das Unternehmen ist jedoch nicht völlig frei darin, wie es die Abmeldung von einem Werbe-Newsletter gestaltet. Zwar enthält die DS-GVO keine ausdrückliche Regelung über die Abmeldung von Newslettern, also den Widerruf der zuvor erklärten Einwilligung in den Erhalt des Newsletters. Allerdings ist hierbei insbesondere Art. 7 Abs. 3 Satz 4 der DS-GVO zu beachten, wonach – auf den Newsletter übertragen – eine Abmeldung nicht komplizierter als die vorherige Anmeldung sein sollte (so auch die Datenschutzkonferenz in Ziffer 3.7. der Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung vom Februar 2022).

Daneben gelten natürlich auch hier die allgemeinen Vorschriften von Art. 5, 12 und Art. 25 DS-GVO, wonach alle Verfahren möglichst betroffenenfreundlich, einfach, selbsterklärend und datensparsam sein sollen.

Daraus leiten wir die Pflicht einer verantwortlichen Stelle ab, dass

1. die betroffene E-Mail-Adresse nach Anklicken des Abmeldelinks im Newsletter bereits auf der für die Abmeldung vorgesehenen Landing-Page (Abmeldeseite) steht und –

2. wenn es schon Auswahlfelder geben soll – das Feld „vollständige Abmeldung“ als erste Option aufgeführt wird und vorausgewählt sein muss, damit die Betroffenen mit nur einem weiteren Klick, schnell und einfach, die vollständige Abmeldung vom Newsletter durchführen können. Schließlich haben sie auch genau deswegen den Abmeldelink im Newsletter angeklickt.

Um den Betroffenen zu bestätigen, dass die Abmeldung erfolgreich war, sollten sie im Anschluss auf eine Bestätigungsseite weitergeleitet werden (z. B.: „Sie sind jetzt vom XY-Newsletter abgemeldet.“). Dies haben wir so diesem Unternehmen mitgeteilt – und es hat dann auch das Verfahren entsprechend kundenfreundlich abgeändert.

Unternehmen sollten bei der Abmeldung von einem Newsletter keine Hürden aufbauen, sondern eine schnelle, einfache und übersichtliche Abmeldung sicherstellen.

☛ Weitere Informationen

Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung vom Februar 2022:
datenschutzkonferenz-online.de/media/oh/OH-Werbung_Februar%202022_final.pdf

Datenschutzrechtliche Aspekte bei der Dokumentation von Flügen unbegleiteter Minderjähriger

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

Durch einen Hinweis wurden wir auf eine Thematik aufmerksam gemacht, mit der sich unsere Dienststelle bislang noch nicht befassen musste: Die reichlich ungeschützte Dokumentation von Flügen unbegleiteter Minderjähriger, sog. „UM“ (Unaccompanied Minors), auf einem Flughafen in Baden-Württemberg durch die zuständige Flughafengesellschaft.

Kritisch fiel uns zunächst das uns vom Hinweisgeber übermittelte Formular „Auftragsannahme UM Boarding Support“ der Flughafengesellschaft auf:

Datenschutzrechtliche Aspekte sind zu beachten bei der Dokumentation von Flügen unbegleiteter Minderjähriger.

Dieses Formular war so aufgebaut, dass in Form einer Tabelle die jeweiligen Daten eines UM in einer Reihe bzw. Zeile eingetragen werden mussten. Die Daten des nächsten UM waren eine Zeile tiefer einzutragen. Dabei handelte es sich um folgende Datenkategorien: Flugnummer, IATA-Airline-Code, Anzahl, Name des UM, Unterschrift Besatzungscrew, Unterschrift Gate-Mitarbeiter_in, Unterschrift Abholer_in, Passnummer Abholer_in.

Infokasten

Unbegleitete Minderjährige (manchmal auch „unbegleitete Kinder“ oder „getrennte Kinder“ genannt) sind Kinder, die auf einem gewerblichen Flug, in einem Zug, einem Bus oder im Rahmen einer ähnlichen Beförderung ohne Anwesenheit eines gesetzlichen Vormunds (= einer erziehungsberechtigten Person, also beispielsweise ohne Eltern) reist. Jedes Jahr reisen viele Kinder allein, um z. B. an Sprachschulen, Sommerlagern oder Schüleraustauschprogrammen teilzunehmen. Auch getrenntlebende Eltern oder Familienmitglieder im Ausland machen es regelmäßig notwendig, den eigenen Nachwuchs allein auf die Reise zu schicken und ihn für eine kurze Zeit in fremde Hände zu geben. Einige Kinder müssen nach einer Krisensituation, in die ihre Eltern verwickelt sind, oder zu Umsiedlungszwecken allein reisen.

Die meisten Fluggesellschaften verfügen über spezielle Betreuungs-Programme für unbegleitete Minderjährige, die zusätzlich zur Flugreservierung kostenpflichtig gebucht werden können: So dürfen z. B. bei der Lufthansa Kinder im Alter zwischen 5 und 11 Jahren nur alleine fliegen, wenn sie den speziellen Lufthansa-Betreuungsdienst in Anspruch nehmen oder zusammen mit einer Person reisen, die mindestens 12 Jahre alt ist. Auch für allein reisende Kinder im Alter von 12 bis maximal 17 Jahren kann dieser Betreuungsservice seitens der Eltern gebucht werden.

Dieser Formularaufbau führte natürlich dazu, dass jede_r Ausfüllende auch alle Angaben der anderen eingetragenen Kinder lesen konnte, was datenschutzrechtlich natürlich als Datenoffenbarung an Unberechtigte unzulässig war. Dieser missliche Umstand wog besonders schwer, da die Daten von Kindern besonders schützenswert sind (vgl. ErwGr. 38 der DS-GVO).

Hinzu kam, dass auf diesem Formular keinerlei Datenschutzhinweise zu finden waren; auch in der allgemeinen Datenschutzhinweisen dieser Flughafengesellschaft kam diese Dokumentation der UM nicht vor.

Weitere Kritikpunkte waren die Aufbewahrung der Formulare und die Einhaltung der Zugriffsberechtigungen.

Im Rahmen eines durchgeführten Kontrollverfahrens wurde die Flughafengesellschaft auf diese datenschutzwidrigen Umstände hingewiesen und zur Abhilfe aufgefordert.

Die Gesellschaft zeigte sich einsichtig und äußerst kooperativ und stellte das Verfahren entsprechend unserer Vorgaben um. Nunmehr wird für jede_n unbegleitete_n Minderjährige_n ein eigenes Formular verwendet. Auch die Themen Aufbewahrung, Zugriffsberechtigungen und Datenschutzhinweise wurden entsprechend umgesetzt.

☛ Weitere Informationen

Informationsseite der Lufthansa zur Alleinreise von Kindern:
www.lufthansa.com/de/de/alleinreisende-kinder

Der geschwätzige QR-Code – Ungewollter Datentransfer per Transaktionsfreigabeverfahren im Online-Banking

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

QR-Codes (QR für „quick response", also „schnelle Antwort") sind praktisch, modern – und für Menschen nicht lesbar. Die hierdurch entstehende Intransparenz kann gerade im Finanzbereich mit Gefahren für die Nutzenden verbunden sein.

Eine Bank im Land bot ihrer Kundschaft ein App-basiertes Freigabeverfahren für Online-Transaktionen an. Zur erstmaligen Aktivierung dieses Verfahrens bzw. zur Registrierung des Geräts (Smartphone, Tablet, PC) übersandte die Bank ihren Kund_innen einen Brief, in dem neben einem alphanumerischen Aktivierungscode auch ein QR-Code abgedruckt war. Dieser enthielt die für die Nutzung des Freigabeverfahrens benötigten Kund_innendaten, insbesondere eine Benutzendenkennung, die sich aus einer die Bank bezeichnenden Kennziffer und der Kund_innennummer zusammensetzte. Letztere war mit der jeweiligen Girokontonummer identisch.

Die Kund_innen sollten mit Hilfe der Banking-App den QR-Code aus dem Brief scannen und auf diese Weise ihre personenbezogenen Daten für das Freigabeverfahren zur Verfügung stellen, ohne sie händisch in die App eingeben zu müssen. Alternativ konnten die Benutzendenkennung und der Aktivierungscode manuell eigegeben werden. Eine URL (Uniform Ressource Locator, „einheitlicher Ressourcenverorter", kurz: Adresse) einer Internetseite war ebenfalls im QR-Code enthalten.

Im konkreten Fall verwies diese URL jedoch aufgrund eines Versehens auf eine Internet-Domain, die sich nicht im Besitz der Bank oder eines von ihr beauftragten Unternehmens befand. Wer auch immer die Domain tatsächlich besaß, erhielt daher, wenn ein_e Kund_in das Freigabeverfahren nicht über die Banking-App aktivierte, sondern mittels QR-Reader und Browser diese Internetseite direkt aufrief, regelmäßig den Aktivierungscode und die Benutzendenkennung.

Da die Girokontonummer in der Benutzendenkennung enthalten war, hätte der auf der besagten Internetseite nunmehr angehäufte Datenbestand etwaigen Angriffen Tür und Tor geöffnet. Insbesondere lässt sich bei Kenntnis der Kontonummer und der kontoführenden Bank die zum Konto gehörende Internationale Bankkontonummer (Inter-

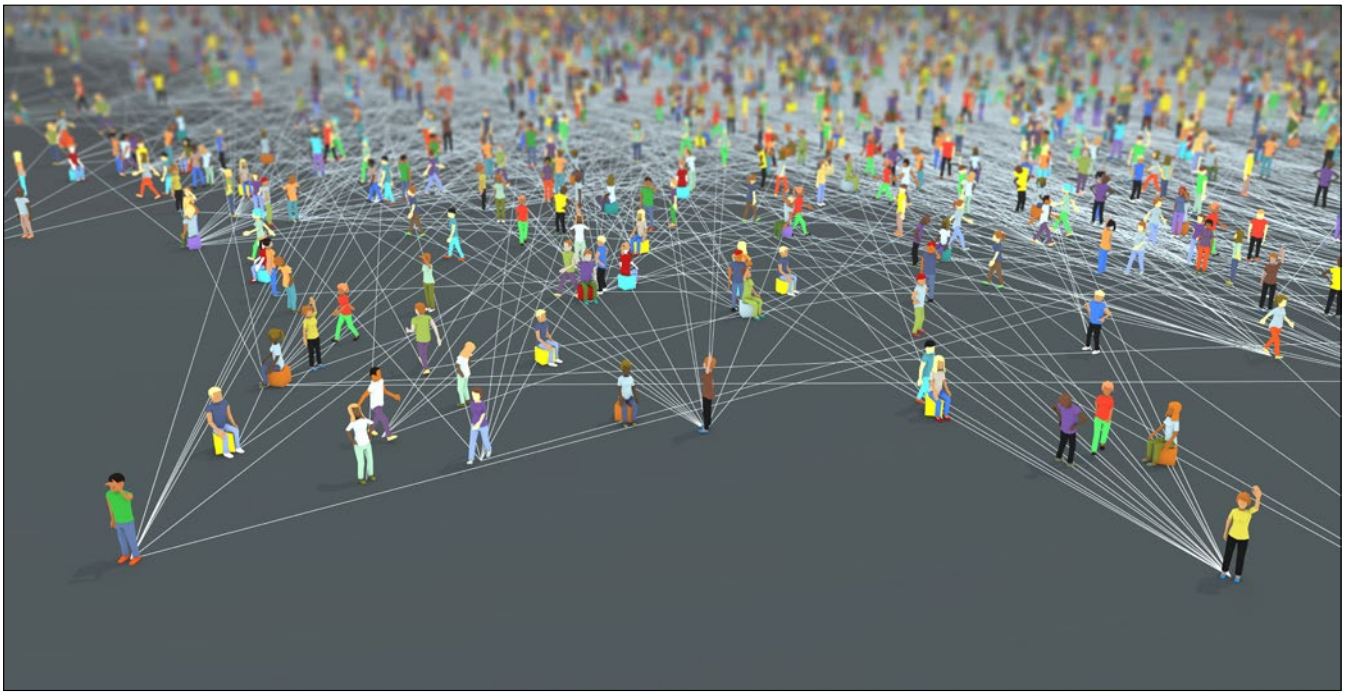
national Bank Account Number – IBAN) ermitteln und z. B. für ungenehmigte Abbuchungen missbrauchen. Aufgrund der Häufung der Unzulänglichkeiten haben wir die Bank gemäß Art. 58 Abs. 2 Buchst. b) DS-GVO verwarnt.

Die Banken, die dieses Verfahren einsetzten, hatten großes Glück, dass ein Sicherheitsforscher diese Schwachstelle zuerst entdeckte und die Domain auf sich registrierte, bevor Kriminelle mithilfe einer gefälschten Internetseite zusätzlichen Schaden durch Abfischen von Informationen, Umleitung auf andere Internetseiten sowie Schadsoftware anrichten konnten.

Die Kund_innen der Bank können dem ihnen übersandten QR-Code nicht unmittelbar ansehen, welche sie betreffenden Daten darin enthalten sind und wer diese Daten bei Aktivierung des Freigabeverfahrens erhält. Die verantwortliche Bank sollte daher insoweit für Transparenz sorgen:

- Das Anschreiben, mit dem ein personenbezogener QR-Code versandt wird, sollte die in diesen eingebetteten Datenkategorien im Klartext nennen.
- Ebenso sollte die im QR-Code enthaltene URL, an die die Daten bei Aktivierung des Freigabeverfahrens übermittelt werden, ausdrücklich angegeben werden. Nur so können die Kund_innen (und auch die handelnden Bankmitarbeitenden) die Richtigkeit der URL überprüfen, indem sie diese vor der Aktivierung des Freigabeverfahrens in ihren Webbrowser eingeben.

Dass eine Internetseite, die dafür ggf. verwendet wird, sich auch im Kontrollbereich der Bank befinden sollte, versteht sich. Warum das bei einer obligatorischen Qualitätsprüfung vor Produktivsetzung nicht auffiel, konnte bankseitig leider nicht aufgeklärt werden. Auch bei Nutzung von QR-Codes sind die personenbezogenen Daten der Kund_innen stets in einer für sie transparenten Weise zu verarbeiten.



Der LfDI befasst sich immer wieder mit Fragen zum Tracking im Internet.

Abteilung 5: Technisch-organisatorischer Datenschutz, Datensicherheit

Anmeldezwang für Geräte

✎ Art. 57 Abs. 1 Buchst. f) DS-GVO

Zugriff auf Ihr Gerät von überall. So lautet das Versprechen vieler Anbieter, wenn sie versuchen, Kunden von einer Kundenkonto-Anmeldung zu überzeugen. Solche Kundenkontos ermöglichten den Zugriff auf aktuelle Informationen über verbundene Geräte und auch schnellen und produktspezifischen Support, falls das Gerät mal nicht richtig funktioniere. Hinter diesen sehr nützlichen Vorteilen verbergen sich jedoch viele Risiken, insbesondere dann, wenn auf der Webseite, auf der man sich ein Kundenkonto anlegt und das entsprechende Gerät registriert, Tracking betrieben wird.

Uns erreichte eine Beschwerde, die einen mutmaßlichen Anmeldezwang für ein Gerät zum Gegenstand hat. Wir haben daraufhin die Webseite zur Anmeldung genau unter die Lupe genommen. Dabei stelle sich raus, dass bereits ohne eine Interaktion durch den Nutzenden auf der Webseite Verbindungen zu verschiedenen Drittanbieter-Servern durchgeführt werden. Auch eine Vielzahl von Cookies wurden bereits gesetzt, bevor sich der Nutzende sich über mögliche Verarbeitungen aus dem Einwilligungsbanner informieren konnte. Entsprechende Informationen zu den jeweiligen Cookies waren den Nutzenden dabei nicht zugänglich.

Tracking im Web

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

Eine Beschwerde hat uns dazu angeregt, hier nun einige kurze, allgemeine Ausführungen zu einem Thema zu formulieren, welches uns künftig möglicherweise häufiger begegnen wird: Gekaufte Produkte müssen online registriert werden, bevor sie genutzt werden können. Dabei kann es vorkom-

men, dass im Zuge der Registrierung unrechtmäßig Tracking eingesetzt wird. Zum Teil werden dutzende Cookies und ähnliche Technologien bereits vor dem Einwilligungsbanner gesetzt. Geräte-Daten aus dem Browser ausgelesen, Übermittlungen an Server verschiedener Drittanbieter finden statt, das heißt also: Es kann vorkommen, dass Sie ein Produkt kaufen und für die Registrierung des Produkts Drittanbietern Ihre personenbezogenen Daten abgeben. Ist das notwendig? Aus datenschutzrechtlicher Sicht kann es schnell zum Problem werden für den Website-Anbieter, wenn er unerlaubt Tracking einsetzt.

Weil Tracking ein sehr umfangreiches Thema ist, haben wir eigene FAQ hierzu erstellt. Diese haben wir in unserem Bildungszentrum BIDIB vorgestellt, Schulungen dazu angeboten. Wir erläutern sie in für Verantwortliche verständlicher Sprache und zeigen darin unsere Ansichten mit konkreten Beispielen zu Standardfehlern. Die FAQ nehmen wir auch als Referenz für unsere Prüfungen.

Bei Tracking handelt es sich meistens um einen komplexen und umfangreichen Sachverhalt. Deshalb prüfen wir die einzelnen Verarbeitungsprozesse, wie etwa das Ablegen eines konkreten Cookies oder die Übermittlung einer konkreten Information.

Eine solche Verarbeitung unterliegt zweierlei Regelungsregimen. Während die DS-GVO dem Schutz personenbezogener Daten dient, regelt das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) in § 25 den Einsatz von Cookies und ähnlichen Technologien, mittels derer Informationen auf Endeinrichtungen gespeichert oder aus diesen ausgelesen werden – und zwar unabhängig davon, ob diese personenbezogen sind oder nicht. Das TDDDG schützt also vor allem die Privatsphäre der Endeinrichtungen bzw. schützt sie vor Fremdzugriff. Vergleichbar ist das TDDDG insoweit mit der Unverletzlichkeit der Wohnung (Art. 13 GG), die vor unbefugtem Zutritt schützt. Die sich an den Zugriff anschließende Verarbeitung personenbezogener Daten, z. B. zur Profilbildung der Nutzenden, wird vom TDDDG dagegen nicht erfasst. Sie unterliegt vollständig der DS-GVO, die den Umgang mit personenbezogenen Daten regelt.

Der Einsatz von Cookies und ähnlichen Technologien ist nicht per se unzulässig. Zur ordnungsgemäßen Anzeige einer Webseite spielen sie eine nicht zu unterschätzende Rolle. So speichern sie Informationen über die grundlegende Einstellung des Nutzenden wie etwa die Sprach- oder Regionseinstellung, über die gespeicherten Artikel im Warenkorb usw. In solchen Fällen unterfällt ihre Nutzung der in § 25 Abs. 2 TDDDG vorgesehenen Ausnahme. Gemäß § 25 Abs. 1 Satz 1 TDDDG bedarf die Speicherung von Informationen wie Cookies in der Endeinrichtung oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, grundsätzlich der Einwilligung der Nutzenden.

Von dem Grundsatz der Einwilligungsbedürftigkeit sind in § 25 Abs. 2 TDDDG Ausnahmen vorgesehen. Für den Zweck eines Trackings von Nutzenden mittels Cookies bzw. ähnlicher Techniken wie Web Storage, Web-Bugs oder Browser-Fingerprinting, finden diese gesetzlichen Ausnahmen keine Anwendung, denn diese sind „nicht erforderlich“, um den vom Nutzenden ausdrücklich gewünschten digitalen Dienst bereitzustellen.

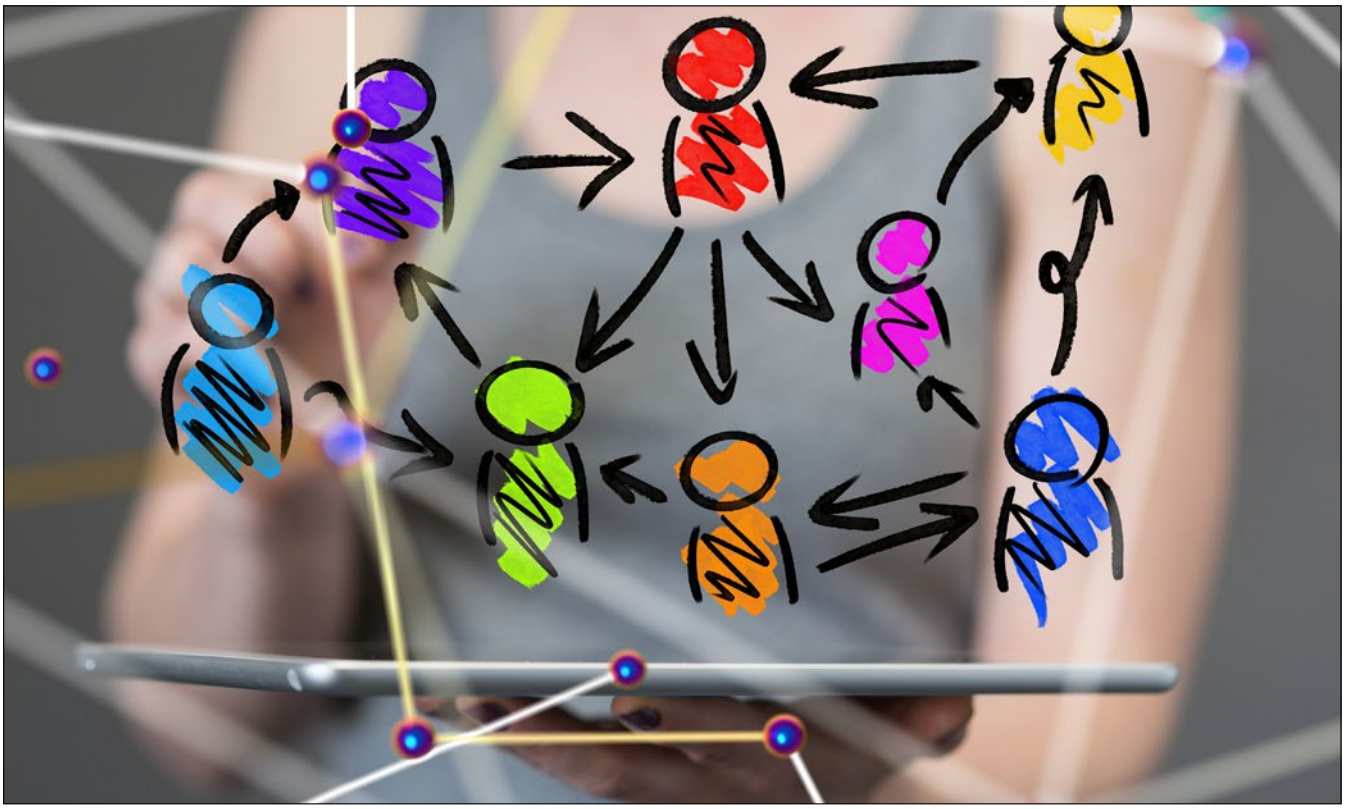
Im Rahmen unserer Tätigkeit stellen wir öfter fest, dass Daten aus dem Endgerät des Nutzenden ausgelesen und zurück an den Server des Webseitenbetreibers übermittelt werden. Zu diesen Daten gehören u. a. konkrete Kennungen, die der Webseitenbetreiber zuvor mittels Cookies und ähnlicher Technologien auf dem Endgerät des Nutzenden abgelegt hat und aufgrund ihres eindeutigen Personenbezug als personenbezogene Daten im Sinne der Datenschutz-Grundverordnung anzusehen sind. Die Übermittlung solcher Daten muss sich innerhalb des Rechtsrahmen der DS-GVO bewegen und durch eine im Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlage gerechtfertigt sein. Der Webseitenbetreiber muss in diesem Fall darlegen und nachweisen können, welchem Zwecke die jeweilige Übermittlung dient, und inwiefern der Übermittlung eine entsprechende Rechtsgrundlage zugrunde liegt.

Tracking in Apps als weiterer Schwerpunkt unserer Tätigkeit

Nicht nur auf Websites wird munter getrackt, auch App-Anbieter setzen mitunter viel Tracking ein. Wir haben eine App untersucht, die die Verwaltung der registrierten Geräte einfacher machen sollte. Der einfache Zugang zu den wichtigen Informationen aller Geräte wird groß beworben. Und genauso einfach fließen auch Daten an Drittanbieter. Die App bediente sich aus einem Baukasten-System (Software Development Kit, kurz: SDK). Dies geschieht häufiger bei App-Anbietern, vermutlich um schnell und kostengünstig eine App zu entwickeln. Unsere Untersuchung mehrerer Apps in diesem Zusammenhang ergab ein trübes Bild: Häufig wurde das SDK eines großen Anbieters genutzt, ohne darauf zu achten, dass dieses bereits bei der Initialisierung der App Informationen aus dem mobilen Endgerät ausliest und diese Daten an diesen Anbieter übermittelt.

So werden auch weitere Elemente dieses Baukasten-Systems genutzt, um z. B. A / B-Testing zu treiben oder Absturz-Berichte zu übermitteln. An sich sind dies legitime Zwecke, um dem App-Anbieter notwendige Informationen zu geben, wie sich die Nutzenden zu den jeweiligen Funktionen der App verhalten, oder im Falle eines Absturzes der App den Fehler zu reproduzieren, um die genaue Ursachen des Absturzes herauszufinden. Es ist unserer Ansicht nach aber regelmäßig nicht notwendig, um einen von den Nutzenden ausdrücklich gewünschten digitalen Dienst zur Verfügung zu stellen (vgl. § 25 TDDDG). Zumal es andere, trackingfreie Alternativen gibt, A / B-Testing zu betreiben oder Absturz-Berichte zu schicken. Solche Dienste sind daher üblicherweise nicht rechtskonform einsetzbar, es sei denn, es wurde vorab zusätzlich eine weitere informierte und freiwillige Einwilligung für die Nutzung des jeweiligen Dienstes eingeholt, die alle Bedingungen für Einwilligungen erfüllt.

Wenn ein Dienst, oder das SDK selbst, beispielsweise umfangreiche Geräteinformationen ausliest, die Rückschlüsse auf eine eindeutig identifizierbare Person erlauben, und sie an eigene Server übermittelt, er Analytics-Funktionen bereitstellt, um Nutzungsverhalten zu analysieren, geht dies i.d.R. mit der Verarbeitung personenbezogener Daten einher.



Auch in In-App-Browsern wird mitunter getrackt.

Auch für diese Verarbeitung ist eine Rechtsgrundlage nach DS-GVO erforderlich, oder der Verantwortliche muss auf diese Verarbeitung verzichten. Dies gilt auch, wenn nicht das SDK Analytics-Funktion betreibt, sondern die App-Anbieter selber Daten zu Analytics-Zwecken an den eigenen Server übermitteln. In beiden Fällen kommt als Rechtsgrundlage grundsätzlich nach DS-GVO nur die Einwilligung in Betracht. In solchen Fällen prüfen wir in einem Schritt, ob die Einwilligung wirksam durch das entsprechende Einwilligungsbanner eingeholt wurde. Zu den häufigsten Fehlern, die wir bei einer App-Prüfung bemängeln, gehört die Nichteinhaltung des Grundsatzes der Vorherigkeit (vgl. unsere Tracking-FAQ Frage 4.2). App-Anbieter müssen sicherstellen, dass keine einwilligungsbedürftige Verarbeitung stattfindet, bevor die Nutzerin oder der Nutzer die Möglichkeit hat, eine informierte und freiwillige Einwilligung in diese Verarbeitung abzugeben.

Tracking-Potenzial durch In-App-Browser

Eine besondere Gefahr stellt die Nutzung des sog. In-App-Browsers dar. Darunter versteht sich ein spezieller Browser, der sich über die App öffnet, wenn der Nutzer auf einen Link in der App tippt. Für viele Nutzende ist eine solche eigene Web-Ansicht innerhalb der App besonders bequem: Sie müssen die gerade im Einsatz befindliche App nicht verlassen und können einfach wieder zur vorherigen Ansicht zurück. Der App-Browser birgt jedoch ein erhebliches Potenzial, Nutzende und ihr Surf-Verhalten zu verfolgen.

In diesem Jahr haben wir eine beliebte App aus dem Bereich Soziale Medien auf ihr Tracking-Verhalten in ihrem In-App-Browser untersucht. Wir konnten feststellen, dass, sobald eine externe Seite innerhalb der App aufgerufen wird, der In-App-Browser umfangreiche Daten an den App-Anbieter sendet. Dieses Datensendeverhalten ist besonders problematisch, da die Daten mit einer Nutzerin oder einem Nutzer verknüpft werden können. In unserer Messung waren die Daten die vollständige URL, die nach dem Ausfüllen eines Formulars an den Webseitenbetreiber gesendet wurden. Diese URL enthält sämtliche Daten, die die Nutzenden vorher ins Formular eingetragen haben. Durch unsere Messung konnten wir ebenfalls eindeutig feststellen, dass diese Informationen an einen Server des App-Anbieters übertragen werden, der den Verlauf detailliert protokolliert und gleichzeitig mit der Benutzer-ID der Nutzenden verknüpft. Darüber hinaus werden die übertragenen URLs ebenfalls lokal im Rahmen der App gespeichert. In einer Datei im Endgerät sind sowohl der vollständige Aufruf als auch alle vorherigen Aufrufe hinterlegt.

App-Tracking stellt eine zunehmend große Herausforderung dar

Immer mehr Unternehmen bieten ihrer Kundschaft eine App an, sei es zur Verwaltung der Bestellungen, oder zur Fernsteuerung eines Geräts, bis hin zu exklusiven Vorteilen für treue Kund_innen auf dem eigenen Marktplatz. Mit Stand Januar 2025 wurden im Google Play Store 2,1 Mio., im Apple App Store etwas über 2,0 Mio. Apps angeboten. Der Markt für Apps wird größer, und das Geschäft mit den Daten der Kundschaft lukrativer. Für Nutzende bringt die Nutzung einer App viele Vorteile mit sich, birgt allerdings auch viele datenschutzrechtliche Risiken.

Aus Sicht eines Nutzenden ist es schwieriger, in das Datensendeverhalten einer App Einsicht zu nehmen. Um die Datenflüsse einsehen und nachvollziehen zu können, sind oftmals zusätzliche (und mit Kosten verbundenen) Tools erforderlich. Anders als im Web-Browser, in dem gespeicherte Daten durch eine gezielte Löschung der Browser-Daten einfach und sicher entfernt werden können, gestaltet sich eine effektive Löschung der durch die App abgelegte Daten deutlich schwieriger. Im Bereich Web-Browser gibt es verschiedene Open-Source-Lösungen, mit denen effektiv das Tracking unterbunden wird, und nur unbedingt erforderliche Cookies und ähnliche Technologien zugelassen werden. Eine vergleichbar effektive Lösung für Apps ist uns zum Zeitpunkt des Verfassens dieses Beitrags nicht bekannt.

☛ Weitere Informationen

Anzahl der verfügbaren Apps in den Top App-Stores im Januar 2025:
de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores

Standortbasierte Benachrichtigungen in digitalen Eintrittskarten

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

Im Jahr 2024 ging bei uns eine Beschwerde ein, die sich mit einer digitalen Eintrittskarte für den Breitenauer See im Apple Wallet-Format befasste. Die betroffene Person berichtete, dass bei Annäherung an den See automatisch eine Benachrichtigung auf ihrem Gerät ausgelöst wurde, obwohl sie hierfür keine explizite Zustimmung gegeben habe. Diese Benachrichtigungen entstanden durch Standortdaten, die in der pkpass-Datei der Eintrittskarte hinterlegt waren, und führten beim Nutzer zu erheblichen Bedenken hinsichtlich der datenschutzrechtlichen Konformität. Die betroffene Person äußerte die Vermutung, dass diese Funktion einem nicht abschaltbaren Standort-Tracking gleichkomme und kritisierte, dass keine Option zur Deaktivierung oder Abwahl dieser Funktion bereitgestellt wurde.

Funktion und Speicherung von Standortdaten in pkpass-Dateien

Nach eingehender Untersuchung stellten wir fest, dass die Benachrichtigung auf einer Funktion des Apple Wallet-Datenformats pkpass beruht, die im Bereich „locations" des JSON-Datenformats gespeicherte Standortinformationen nutzt. Hierbei handelt es sich nicht um Tracking im klassischen Sinne, sondern um eine lokale Benachrichtigungsfunktion. Die JSON-Datei enthält eine „locations"-Sektion, in der Geokoordinaten (Breiten- und Längengrad) gespeichert sind. Diese Geodaten ermöglichen es, ortsspezifische Hinweise auszugeben, wenn das Endgerät einen bestimmten Standort erreicht. Typische Attribute in diesem Abschnitt sind „latitude" und „longitude" zur Definition der Koordinaten sowie ein Attribut „relevantText", der die Nachricht enthält, die dem Nutzenden in der Nähe des entsprechenden Standortes angezeigt wird.

Diese Funktion bietet Entwickler_innen die Möglichkeit, den Nutzenden gezielte Hinweise zu geben, wenn sie sich in bestimmten geografischen Bereichen aufhalten – ein Mechanismus, der im Marketing, für Kundenbindungsprogramme oder im Veranstaltungsmanagement weit verbreitet ist. In diesem Fall führte die programmierte Geodaten-Funktion dazu, dass bei Annäherung an den Breitenauer See ein Benachrichtigungshinweis angezeigt wurde.

Datenschutzrechtliche Bewertung

Da die Funktion der Benachrichtigung lokal auf dem Gerät des Nutzenden ausgeführt wird, erfolgt dabei keine Übertragung von Standortdaten an externe Server oder an Dritte, wie beispielsweise den Anbieter der Eintrittskarte oder eine andere Instanz. Tracking, im datenschutzrechtlichen Sinne, setzt die Erhebung und Weitergabe von Verhaltensdaten voraus, oft ohne Kenntnis oder Zustimmung der betroffenen Personen. In diesem Fall jedoch beschränkt sich die Funktion darauf, auf dem Endgerät selbst ortsbezogene Hinweise zu geben, ohne dass persönliche Informationen an weitere Stellen weitergeleitet werden. Die Standortbenachrichtigung kann somit als Komfortfunktion betrachtet werden, die dem Nutzenden auf Basis lokaler Daten kontextabhängige Informationen liefert.

Reaktion des Betroffenen und weitere Erläuterungen zur Deaktivierung

Der Betroffene reagierte auf unsere Erläuterung mit Verständnis für die technische Funktionsweise, äußerte jedoch weiterhin die Befürchtung, dass eine solche Benachrichtigung als unfreiwilliges „Tracking" empfunden werde, da er diese Funktion nicht selbstständig deaktivieren könne. In unserer abschließenden Antwort legten wir nochmals dar, dass die Benachrichtigung lediglich dem Hinweis auf die Nähe eines bestimmten Ortes dient und die Informationen auf dem Gerät verbleiben, ohne dass eine Kommunikation mit externen Servern stattfindet. Die Einstufung als „Tracking" wäre nur dann gegeben, wenn diese Standortdaten übermittelt würden, was hier nicht der Fall ist.

Da diese Art der Standortbenachrichtigung in Apple Wallet nicht deaktiviert werden kann, wurde vorgeschlagen, dass Nutzende in den Apple Wallet-Einstellungen oder den allgemeinen Systemeinstellungen die Möglichkeit haben sollten, Benachrichtigungen anzupassen oder vollständig zu deaktivieren.

Das Tracking durch Smartphones kann auch im Rahmen von Veranstaltungen problematisch sein.

Fazit und Einordnung

Dieser Fall verdeutlicht, wie schnell Datenschutzfragen bei modernen, mobilen Technologien zu Missverständnissen und Unsicherheiten führen können. Die genaue Kenntnis der Funktionsweise und der rechtlichen Einordnung trägt jedoch zur Klärung bei und hilft, technische Abläufe von datenschutzrechtlich relevanten Praktiken zu unterscheiden. Mit dieser Untersuchung und den ergänzenden Hinweisen konnten die Datenschutzbedenken adressiert und aufgezeigt werden, dass die Funktionsweise der .pkpass-Datei im Einklang mit den datenschutzrechtlichen Vorgaben bleibt.

Weitere Spotlights aus dem Netz

✎ Art 57 Abs. 1 Buchst. f) DS-GVO

Livestream und On-Demand-Videos

Das Jahr 2024 zeichnete sich durch eine hohe Anzahl an Beschwerden und Beratungsanfragen aus, die die Übertragung von Video-Inhalten in Echtzeit im Internet (Livestream) zum Gegenstand haben. Auf vielen Plattformen wird die Möglichkeit angeboten, die Livestreams später als On-Demand-Videos auf der Plattform zu speichern. In diesen Videoaufnahmen wird mitunter die Öffentlichkeit erfasst, darunter personenbezogene Daten wie das Gesicht einer Person oder das Kfz-Kennzeichen. Für diese On-Demand-Videos müssen sich Verantwortliche mit uns als Aufsichtsbehörde auseinandersetzen.

Für unsere datenschutzrechtliche Bewertung ist die Prüfung in verschiedene Vorgänge zu unterteilen: Das Filmen an sich, das Abspeichern oder Archivieren des Videomaterials sowie die Veröffentlichung im Internet. Das Filmen stellt eine Erhebung personenbezogener Daten dar und bedarf somit einer Rechtsgrundlage. Gleiches gilt für das Abspeichern oder Archivieren auf dem eigenen Rechner. Soweit der Verantwortlicher eine natürliche Person ist und das Videomaterial nur zur Ausübung persönlicher oder familiäre Tätigkeiten dient, fällt die Verarbeitung unter die Haushaltsausnahme und fällt somit nicht unter den Geltungsbereich der DS-GVO.

Problematischer stellt sich die Veröffentlichung dieses Videomaterials im Internet dar, denn dadurch

werden personenbezogene Daten einer unbegrenzten Personenanzahl verfügbar gemacht. In solchen Fällen greift die Haushaltsausnahme nicht mehr mit der Folge, dass die DS-GVO anwendbar ist.

In diesen Fällen ist in einem weiteren Schritt zu prüfen, ob die Veröffentlichung eine journalistische Tätigkeit darstellt und der Verantwortliche das Medienprivileg genießt. Der Gesetzgeber regelt mit dem Medienprivileg, dass das hohe Gut der Pressefreiheit sich der Kontrolle durch eine staatliche Stelle, die wir sind, weitgehend entzieht. Das Privileg gilt für Rundfunkanstalten, Anbieter von journalistischen digitalen Diensten (Webseitenbetreibern) und auch der gedruckten Presse. Der Europäischer Gerichtshof legt den Begriff „journalistische Tätigkeit“ weit aus und lässt daher die Privilegierung auch Blogger_innen zu Gute kommen. Dies hat zur Folge, dass die DS-GVO eingeschränkt anwendbar ist, also nicht für redaktionelle Inhalte, sondern nur hinsichtlich der technischen-organisatorischen Maßnahmen.

Diese eingeschränkte Anwendung der Verordnung bedeutet jedoch nicht, dass Veröffentlichungen keine rechtlichen Grenzen beachten müssen. Persönlichkeitsrechtsverletzungen durch solche Veröffentlichungen sind vielmehr im Rahmen der allgemeinen zivil- und strafrechtlichen Vorschriften zu werten. Entsprechende Vorschriften bleiben unberührt.

In anderen Fällen, in denen der Verantwortliche sich nicht auf das Medienprivileg berufen kann, muss er die Verarbeitung auf einer Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO stützen können; andernfalls ist die Verarbeitung unzulässig.

Namensnennung auf Bewertungsportalen

Besonders häufig erreichten uns Beschwerden, die die Nennung des Namens der betroffenen Person auf Bewertungsportalen betrifft. Heutzutage finden sich zu fast allen Dienstleistungen Rezensionen von Kund_innen. Besonders ärgerlich für den Dienstleistungsanbieter ist, wenn ein_e Kund_in auf bekannten Online-Plattform eine negative Bewertung abgibt, die für andere sichtbar ist und somit möglicherweise potenzielle Kundschaft abschreckt. Aus diesem Grund reagieren viele Dienstleistungsanbieter auf negative Bewertungen von Kund_innen empfindlich und nehmen zu den dort genannten Vorwürfen Stellung. Und um die Antwort noch persönlicher zu machen, schreiben viele von ihnen noch den Namen der Person in einer persönlichen Anrede dazu, auch wenn die Bewertung unter einem Pseudonym geschrieben wurde. Dabei vergessen sie jedoch, dass die Nennung des klaren Namens der Kund_innen eine Verarbeitung personenbezogener Daten ist und somit einer Rechtsgrundlage nach Art. 6 Abs. 1 Buchst. a) DS-GVO bedarf.

Da die Bewertung in den uns erreicht habenden Fällen unter einem Pseudonym abgegeben wurde, ist nicht von einem Willen der betroffenen Person auszugehen, ihren Namen auf einer öffentlichen Plattform für andere Nutzende kenntlich zu machen. Auch ein überwiegendes berechtigtes Interesse nach Art. 6 Abs. 1 Buchst. f) DS-GVO kommt nicht in Betracht. Für den Dienstleistungsanbieter ist zwar denkbar, dass das Interesse, die Person, die ihn schlecht bewertet, mit Gegenargumenten zu konfrontieren, um anderen Nutzenden ein vollständiges Bild der Situation zu geben, ein berechtigtes Interesse ist. Dieses Interesse überwiegt jedoch in den uns erreicht habenden Fällen nicht das Interesse der betroffenen Person, ihre Identität und somit eine Geschäftsbeziehung mit dem besagten Dienstleistungsanbieter der Öffentlichkeit preiszugeben. Vor diesem Hintergrund haben wir in diesen Fällen den Verantwortlichen direkt aufgefordert, den Namen der betroffenen Person aus der Antwort zu entfernen.

© kwasibanane

Cookies sind nicht immer schlecht.

Gute und nicht so gute Cookies

2024 erreichte uns auch eine Vielzahl an Beschwerden, die die Cookies-Praxis verschiedener Webseiten-Betreiber bemängeln. Manche Webseiten-Betreiber geben selbst an, dass sie unterschiedliche Cookies einsetzen; jedoch fehlen genauere Angaben dazu, welches Cookie zu welchem Zweck zu welchem Zeitpunkt eingesetzt wird. Aus der Perspektive der Verbraucher_innen sind diese notwendigen Informationen solchen pauschalen Angaben nicht zu entnehmen.

Wir haben uns auf die Suche gemacht und konnten in vielen Fällen feststellen, dass Cookies, die beim Besuch einer Internetseite gesetzt werden, und noch bevor Nutzende mit dem Einwilligungsbanner interagieren, technisch erforderlich und somit „harmlos" sind. Entgegen der in der Praxis weit verbreiteten Annahme ist der Einsatz von Cookies nicht per se rechtswidrig. Datenschutzrechtlich ist es nicht sofort unzulässig, Cookies zu setzen. Das Hypertext Transfer Protocol (HTTP), das Protokoll, das zur Übertragung von Webseiten verwendet wird, ist ein zustandsloses Protokoll auf Anwendungsebene. Dies bedeutet, dass jede Anfrage, die Nutzende an den Webserver schicken, eine eigene Sitzung darstellt. Der Webserver kann Nutzende nicht wiedererkennen, weil er nach jeder Sitzung alle erhaltenen Informationen löscht. Um die Zustandslosigkeit des HTTP-Protokolls zu umgehen, werden Cookies verwendet. Der Einsatz von Cookies ist zulässig, wenn er unbedingt erforderlich ist, um den ausdrücklich gewünschten Dienst zur Verfügung zu stellen (vgl. § 25 Abs. 2 TDDDG). Wenn also gewünscht ist, dass das Konto im Browser gespeichert bleibt, und ausschließlich zu diesem Zwecke Cookies gesetzt werden, ist deren Einsatz mit dem o. g. rechtlichen Rahmen des TDDDG vereinbar.

Oftmals werden, ohne dass es notwendig ist, personenbezogene Daten erhoben. Das wissen sehr viele Bürgerinnen und Bürger. Daher erreichen uns immer wieder Beschwerden über mutmaßlich rechtswidrige Verarbeitungen. Wo angezeigt, greifen wir dann ein und unterstützen die betroffenen Personen. Insgesamt empfehlen wir verantwortlichen Stellen, dass sie klar und transparent darüber informieren, welche personenbezogene Daten sie verarbeiten und wofür. Dies fördert das Vertrauen in die Verarbeitungsprozesse und die digitale Sphäre insgesamt.

Neues aus der Bußgeldstelle

Allgemeine Bußgeldstelle

Im Berichtszeitraum konnten wir einen deutlichen Anstieg der Eingangszahlen innerhalb der Bußgeldstelle auf 243 (Stand 31.12.2024) verzeichnen. Im Vorjahr waren es noch 185 Verfahrenseingänge. Ein wesentlicher Grund für den Anstieg dürfte sein: Polizeireviere in Baden-Württemberg leiten zwischenzeitlich konsequent Ermittlungen zu Anzeigen über Datenschutzverletzungen ein, um diesen nachzugehen. Beratungsgespräche zeigen, dass bei nachgewiesenen massiven Datenschutzverstößen aufseiten der Polizei wie auch den Bürger_innen die Erwartung vorherrscht, dass diese Verstöße auch konsequent sanktioniert werden. Auch wenn wir weiterhin unserer Linie treu bleiben, zunächst auf Beratung zu setzen und nur in gewichtigen Fällen, bei wiederholten Verstößen oder Uneinsichtigkeit aufseiten des Verursachers zur Sanktion durch Bußgelder zu greifen, wurden im Berichtsjahr zahlreiche Sanktionen ausgesprochen, insgesamt haben wir 53 Bußgeldbescheide mit Bußgeldern in Höhe von ca. 626.700 Euro erlassen.

Gleichfalls wurde aber auch das „Opportunitätsprinzip“ in datenschutzrechtlichen Bußgeldverfahren ausreichend beachtet, sodass geringfügige Datenschutzverstöße nicht geahndet und gem. § 47 Abs. 1 OWiG eingestellt wurden. In einer Vielzahl von Fällen war auf den Privatklageweg zu verweisen, da ein öffentliches Interesse an einer Verfolgung und Sanktionierung nicht vorlag.

Vorgänge, bei denen ein Verstoß nicht nachgewiesen werden konnte, wurden konsequent gem. § 170 Abs. 2 StPO i.V.m. § 46 OWiG eingestellt.

Immer wieder Thema: Videoüberwachung.

In der Gesamtbetrachtung handelte es sich somit im Berichtjahr um 252 erledigte Bußgeldverfahren. Davon umfasst waren auch noch Vorgänge aus den Vorjahren, da manches Verfahren auch über eine längere Zeit bearbeitet wird.

Private Videoüberwachung

Ein großer Teil der Anzeigen, die bei der Bußgeldstelle landen, beinhalten die Thematik der privaten Videoüberwachung. Die überwiegenden Fälle, häufig im Zuge von Nachbarschaftsstreitigkeiten, werden aufgrund einer fehlenden Beweislage hinsichtlich einer tatsächlichen Datenverarbeitung eingestellt. Im folgenden Fall war es jedoch geboten einzuschreiten, da hier ein besonders hoher Grad an Uneinsichtigkeit bestand.

Swimmingpool – Hohes Bußgeld wegen unzulässiger Bildaufzeichnungen

Im Rahmen eines Nachbarschaftskonflikts um ein errichtetes Außenschwimmbad kam es zu einem Bußgeldverfahren gegen den Nachbarn, der heimlich Videoaufnahmen mittels Smartphone anfertigte. Dieser filmte über mehrere Stunden hinweg Badegäste, oftmals ohne deren Wissen. Durch Zurufe des filmenden Nachbars sollten die Badegäste zusätzlich provoziert bzw. animiert werden, sich expressiv zu verhalten, auch wurde einer verbalen Auseinandersetzung nicht aus dem Weg gegangen, die filmisch festgehalten wurde. Eigentliches Ziel der Aufnahmen war die vermeintliche Beweissicherung für eine Klage wegen Lärmbelästigung durch den Betrieb des Außenschwimmbads.

Mit den Videoaufzeichnungen verstieß der „Kameramann“ gegen die DS-GVO, da Insbesondere keine Einwilligungen der gefilmten Personen (Art. 6 Abs. 1 Buchst. a) DS-GVO) vorlagen. Auch das vorgebrachte berechtigte Interesse des Nachbarn (Art. 6 Abs. 1 Buchst. f) DS-GVO) konnte den massiven Eingriff in die Persönlichkeitsrechte der Badegäste nicht rechtfertigen.

Gegen das verhängte Bußgeld legte der Betroffene zunächst Einspruch ein. Vor Gericht argumentierte er damit, dass die Aufnahmen zur Beweisführung notwendig gewesen seien. Insbesondere habe sich eine der weiblichen Personen bereits wiederholt am Pool für den eigenen Social-Media-Kanal abgelichtet, sodass dies als Zustimmung zu seinen eigenen Bildaufzeichnungen zu werten sei. Das Gericht folgte dieser Argumentation nicht und schloss sich der Auffassung der Datenschutzbehörde an, dass diese Bildaufzeichnungen, im Besonderen auch mit Blick auf die leichte Bekleidung der unfreiwilligen Film-Darsteller_innen, nicht nur unzulässig, sondern auch unverhältnismäßig gewesen seien. Das Gericht betonte ausdrücklich, dass weniger invasive Methoden zur Lärmdokumentation ausgereicht hätten, ohne die Privatsphäre der Nachbarn zu verletzen.

Das Gericht ist unserer Rechtsauffassung gefolgt und hat die Person zu einem Bußgeld verurteilt.

Der Fall verdeutlicht die hohen Anforderungen an die Zulässigkeit von Videoüberwachung im privaten Bereich. Auch in Konfliktsituationen müssen datenschutzrechtliche Vorschriften strikt eingehalten werden.

Videoüberwachung in Mannheimer Bordellen

Wiederholt wurde uns durch die Polizei mitgeteilt, dass durch einen „Laufhaus“- und Bordellbetreiber im Mannheimer Rotlichtbereich eine massive private Videoüberwachung im öffentlichen Bereich vorgenommen werde. Im Rahmen einer groß angelegten richterlich angeordneten Durchsuchung konnten in einem öffentlich zugänglichen „Laufhaus“ eine große Anzahl von Videokameras beschlagnahmt werden. Die Kameras befanden sich an unterschiedlichen Gebäudefassaden und waren alle auf den öffentlichen Straßenbereich innerhalb der Bordellbetriebe ausgerichtet. Gleichzeitig wurden auch im Treppenhaus des Gebäudes eine zweistellige Anzahl von Kameras aufgefunden und beschlagnahmt. Die Kameras waren technisch so eingerichtet, dass diese Videodaten in Echtzeit auf drei Großbildschirme im Bewirtschaftungsraum des Gebäudes übertrugen.

Vor Ort führten wir eine Durchsuchung durch unter Einbeziehung der Polizei.

Aus datenschutzrechtlicher Sicht waren folgende Aspekte bei der Bewertung dieser Videoüberwachung zu berücksichtigen, erstens: Die private Videoüberwachung des öffentlichen Bereichs fällt unter die Beschränkungen des Art. 6 Abs. 1 Buchst. f) DS-GVO. Zweitens: Die Zulässigkeit der Überwachung von Beschäftigten richtet sich ausschließlich nach den engen Voraussetzungen des Art. 88 der DS-GVO i. V. m. § 26 des Bundesdatenschutzgesetzes (BDSG). Demnach dürfen gemäß § 26 Abs. 1 S. 2 BDSG personenbezogene Daten von Beschäftigten ausschließlich zur Aufdeckung von Straftaten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Der Betrieb aller Kameras an der Gebäudefassade und im gesamten Treppenhaus des Gebäudes stellte eine automatisierte Verarbeitung personenbezogener Daten der Freier, der potenziellen Kunden, der Prostituierten und weiterer Beschäftigten dar (vgl. EuGH, Urt. v. 11.12.14, C-212 / 13, Leitsatz 2, juris). Zudem war aufgrund fehlender Hinweisbeschilderung zur Datenverarbeitung eine Zuordnung zur verantwortlichen Stelle nicht gegeben.

Ein Abschluss des Verfahrens steht aus. Die Bußgeldstelle wird ihre Arbeit hier fortsetzen und das Verfahren zu Ende führen.

Einsatz von Tracking-Geräten

Gerade im Bereich von Beziehungsstraftaten ist in vielen Fällen ein sog. Tracking-Gerät zur unzulässigen Standortüberwachung von Personen im Einsatz. Wiederholt lässt sich in diesem Jahr eine Zunahme von ausufernden Überwachungsmaßnahmen im familiären Nahbereich feststellen. Im Berichtszeitraum wurden daher durch die Bußgeldstelle für die Polizei aus dem Bereich „Stalking und häusliche Gewalt" mehrere Schulungen angeboten, um für diese sensible Thematik mehr Rechtssicherheit zu vermitteln.

Überwachung in Partnerbeziehungen

So brachte ein von Eifersucht geleiteter Mann unter dem Fahrzeug des angeblichen Nebenbuhlers ein Smartphone am Auspufftopf an. Dieses verband er mit dem eigenen Mobilgerät mittels Bluetooth, um immer die genauen Standortdaten zu bekommen. Bei seiner ehemaligen Lebenspartnerin deponierte er zeitgleich einen sog. Air-Tag in der Handtasche. Vermutlich aufgrund der starken Geräuschentwicklung am Auspuff schaute die observierte Person unter ihrem Fahrzeug nach und entdeckte das Gerät. Eine Polizeistreife nahm sich umgehend des Vorfalls an und betrieb vor Ort eine umfangreiche Beweismittelsicherung. Mit dem Verdacht der unrechtmäßigen Überwachung stritt der Ex-Partner jegliche Überwachungsabsichten ab. Dieser Aussage folgten wir auf Grundlage unserer Erkenntnisse nicht und finalisierten schließlich das Bußgeldverfahren, welches nunmehr rechtskräftig ist.

Auf der Baustelle trotz Krankheitszeit

Auch in der Arbeitswelt hält Tracking immer mehr Einzug. So setzte ein Arbeitgeber im Baugewerbe ein münzgroßes Trackinggerät ein, um den ständigen Standort des offiziell krankgeschriebenen Mitarbeiters angezeigt zu bekommen. Hier bestand nämlich der konkrete Verdacht, dass dieser zwischenzeitlich wieder zu Kräften gekommen sei, da er auf einer anderen Baustelle gesichtet wurde. Um hier Gewissheit zu erlangen, platzierte der Arbeitgeber heimlich einen „Tracker" im Innenraum des privaten Fahrzeugs. Das Ergebnis: Der vermeintlich kranke Arbeitnehmer wurde in flagranti mit Arbeitshandschuhen auf der besagten Baustelle angetroffen.

Auch wenn die Maßnahme sicherlich auf der Ebene persönlicher Betroffenheit nachvollziehbar und mit Blick auf die Offenlegung des Betrugs gerechtfertigt erscheint: „Gerecht" im gesetzlichen Sinne war diese Überwachungsmaßnahme nicht und brachte dem Arbeitgeber ein hohes Bußgeld ein. Nicht nur, dass der arbeitsrechtliche Prozess wegen der ausgesprochenen fristlosen Kündigung gegenüber dem Mitarbeiter mit einem Vergleich und einer hohen Ausgleichszahlung für den Ar-

beitgeber endete; die beiden Unternehmer aus der Baubranche wurden auch mit hohen Bußgeldern wegen des vorliegenden DS-GVO-Verstoßes durch den Einsatz eines Trackinggeräts in diesem Anwendungsfall belegt.

Welche Aspekte waren hier ausschlaggebend? Eine Einwilligung des Mitarbeiters i. S. Art. 6 Abs. 1 Buchst. a) DS-GVO lag unstrittig nicht vor. Selbst wenn der Arbeitgeber ein berechtigtes Interesse an der Aufklärung von Missbrauchsverdacht hatte, so müssen die gewählten Mittel dennoch verhältnismäßig i. S. Art. 6 Abs. 1 Buchst. f) DS-GVO sein.

Das heimliche Tracking stellte einen massiven Eingriff in das allgemeine Persönlichkeitsrecht des Mitarbeiters dar. Arbeitgeber sind gut beraten, im Verdachtsfall auf legale und verhältnismäßige Methoden zur Aufklärung zurückzugreifen, um schwerwiegende rechtliche Konsequenzen wegen eigenen Fehlverhaltens zu vermeiden, aber dennoch das vertragswidrige Verhalten eines Mitarbeitenden ahnden zu können.

Mitarbeiterexzess und kein Ende in Sicht

Missbrauch des polizeilichen Vorgangsbearbeitungssystems

Leider erliegen aber auch immer wieder Polizeibeamt_innen der Versuchung, über die polizeilichen Informations- und Auskunftssysteme eine romantische Beziehung einfädeln zu wollen.

So geriet ein Polizeibeamter in Schwierigkeiten, nachdem er privaten Kontakt zu einer jungen Studentin einer badischen Universitätsstadt über einen bekannten Messenger-Dienst aufnahm. Die Rufnummer hatte er dem polizeilichen Vorgangsbearbeitungssystem (ComVor) entnommen, welche zuvor durch ihn im Rahmen einer Verkehrskontrolle erhoben wurde. Die Betroffene brachte den Fall zur Anzeige.

Der Fall stellt einen klaren Verstoß gegen die DS-GVO sowie gegen die Wohlverhaltenspflichten eines Beamten dar. Die Telefonnummer wurde ausschließlich für dienstliche Zwecke verarbeitet, ihre Nutzung für private Nachrichten widerspricht demnach bereits dem Grundsatz der Zweckbindung.

Auch hatte die weibliche Person zu keinem Zeitpunkt i. S. Art. 6 Abs. 1 Buchst. a) DS-GVO eingewilligt, dass ihre Daten für private Zwecke genutzt werden. Ebenso war kein berechtigtes Interesse i. S. Art. 6 Abs. 1 Buchst. f) DS-GVO feststellbar. Der Fall soll generalpräventiv aufzeigen, dass unprofessionelle Annäherungsversuche durch Polizist_innen nicht nur unangemessen, sondern auch rechtswidrig sind. Der Missbrauch dienstlich erlangter Daten wird konsequent verfolgt, um die Persönlichkeitsrechte der Bürger_innen zu schützen und Vertrauen in staatliche Institutionen zu bewahren. Der Beamte muss nun die Konsequenzen seiner Handlungen tragen – sowohl durch ein ergangenes Bußgeld als auch dienstrechtlich.

Dienstlich erlangte Kontaktdaten missbräuchlich genutzt

Eine ähnliche Konstellation lag bei einem Angestellten einer Sicherheitsfirma vor, der auf einer touristisch stark frequentierten Insel im „schwäbischen Meer“ seinen Dienst verrichtete. Dieser eignete sich gleichfalls die hinterlegte private Handynummer einer Besucherin an, welche diese zuvor auf einem Leihvertrag für ein mobiles Fahrzeug hinterlassen hatte. Noch am gleichen Tag meldete er sich über einen Messenger-Dienst bei der Dame und fragte zielgerichtet nach einem persönlichen Treffen. Bei der Kontaktaufnahme „outete“ sich dieser als „der Security-Mann“ aus dem zurückliegenden Inselbesuch. Es folgten eine arbeitsrechtliche Abmahnung und ein Bußgeld in vierstelliger Höhe.

Datenabgleich bei der Agentur für Arbeit

Darauf, dass sich gemäß dem bekannten Werbeslogan „alle 11 Minuten ein Single neu verliebt“, wollte man in einem uns bekannt gewordenen Fall nicht warten und half auf unzulässige Weise mit der Nutzung der internen Datenbanken bei der Agentur für Arbeit etwas nach.

Offenbar neugierig geworden auf mehr private Informationen, durchsuchte eine Sachbearbeite-

rin nach einem ersten „Dating“ die internen Informations- und Auskunftssysteme der Behörde und glich unmittelbar die ihr gegenüber getätigten Angaben ihres „Dates“ auf dessen Wahrheitsgehalt ab. Bei ihrer Recherche erfuhr sie aber nicht nur das tatsächliche (jüngere) Alter ihrer neuen Bekanntschaft, sondern auch, dass dieser als arbeitssuchend gemeldet war. Besonders problematisch: Die Sachbearbeiterin nahm zudem Einblick in die Krankenakte des Mannes, die sensible Gesundheitsdaten enthält. Bei ihrem nächsten Treffen konfrontierte sie ihn offen mit diesen neuen Informationen. Der Betroffene erstattete Strafanzeige bei der Polizei. Auch hier erging ein hohes Bußgeld.

Auch dieser Fall zeigt, dass sich vermeintlich unbekümmertes Interesse und der Wunsch privater Kontaktaufnahme häufig nicht als Kompliment vom Gegenüber verstanden werden, sondern als Eingriff in die Privatsphäre und damit Verstoß gegen die informationelle Selbstbestimmung. Dies sollte man dringend auch durch eine rosarote Brille nicht aus den Augen verlieren. Der Zugriff auf vertrauliche Daten ist ein sensibles Thema, das strengen rechtlichen Vorgaben unterliegt. Wer diese ignoriert, riskiert nicht nur seinen Arbeitsplatz, sondern auch eine Sanktionierung durch unsere Behörde.

Entsorgung von Datenmüll

Immer wieder erreichen uns Beschwerden und Hinweise, dass Daten falsch entsorgt werden. Unwissenheit, Unachtsamkeit und Gleichgültigkeit, aber auch der Wunsch, Kosten zu sparen für eine ordnungsgemäße Entsorgung durch ein zertifiziertes Unternehmen, spielen möglichwerweise eine entscheidende Rolle. Wenn es um sensible Gesundheitsdaten geht, ist besondere Sorgfalt bei der Vernichtung der Daten vonnöten.

Eine Praxisschließung mit datenschutzrechtlichen Folgen

So erging es einem Gynäkologen, der sich zwischenzeitlich im Ruhestand befindet. Im Rahmen der Auflösung seiner Facharztpraxis wurden sensible Patientinnenunterlagen nicht etwa durch einen zertifizierten Betrieb vernichtet, sondern an den eigenen Bruder weitergegeben, verbunden mit dem Auftrag, diese zu verbrennen. In einer normalen Papiersammeltonne eines öffentlich zugänglichen Mehrfamilienhauses entdeckten Anwohner_innen die ärztlichen Dokumente und alarmierten die Polizei. Durch Zeugenaussagen der behandelten Patientinnen, deren Identitäten durch die Dokumente offengelegt wurden, konnte auch der ehemals behandelnde Arzt ausfindig gemacht werden.

Aufgrund eines vollumfänglichen Geständnisses und nicht anzunehmender Wiederholungsgefahr wurde trotz der Eingriffstiefe dieses Verstoßes das Bußgeld auf einen mittleren vierstelligen Bereich festgelegt.

Derartige Vorfälle bewerteten wir als erheblichen Verstoß gegen die DS-GVO. Hier handelt es sich zum einen um eine rechtswidrige Datenverarbeitung i. S. Art. 5 Abs. 1 Buchst. f) DS-GVO, da hier die Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit nicht gewährleistet („Integrität und Vertraulichkeit“). Gemäß Art. 32 DS-GVO sind datenverarbeitende Betriebe gerade dazu verpflichtet, sensible Daten sicher und datenschutzkonform zu vernichten. Immer wieder kann es vorkommen, dass Betriebe eine lückenlose, fachgerechte und zertifizierte Aktenvernichtung nach DIN 66399 im Rahmen der Rechenschaftspflichten nicht nachweisen können.

Nicht nachvollziehbar ist, dass in zahlreichen Fällen zwar ein Auftragsverarbeitungsvertrag mit einem „Daten-Entsorger“ besteht, aus Kostenersparnisgründen aber betriebsintern weiterhin Sicherheitslücken geduldet werden. Diese Versäumnisse lassen sich dann auch nicht mit strengen Dienstanweisungen gegenüber den Mitarbeitenden schließen.

Vor Augen sollte sich stets geführt werden, dass die unsachgemäße Entsorgung das Risiko der Offenlegung sensibler Gesundheitsdaten birgt, was hohe Bußgelder zur Folge haben kann. Zusätzlich könnten auch Betroffene zivilrechtliche Ansprüche gem. Art. 82 DS-GVO geltend machen.

© kwasibanane

Korrekte Entsorgung ist wichtig.

Offenlegung von Daten

An das Gedicht des Zauberlehrlings fühlten wir uns im Zusammenhang mit der Verwendung eines Messenger-Dienstes als betriebsinternes Kommunikationsmittel erinnert.

Goethes „Zauberlehrling" und der Spuk der offenen ChatGruppe

Eine der Firmenleitung direkt unterstellte Mitarbeiterin hatte die Idee, ergänzend zu der bereits bestehenden, vermeintlich nicht mehr zeitgemäßen und augenscheinlich ungenutzten digitalen Plattform für Prospektverteiler des Unternehmens eine offene Chat-Gruppe bei einem bekannten Messengerdienst zu eröffnen. Damit wollte sie auf einfachem Weg die Austräger_innen schneller erreichen, besser betreuen und zielgruppengerechter kommunizieren. Mit ihrem gut gemeinten Einsatz für das eigene Unternehmen rief sie jedoch – ganz im Sinne Goethes – „Geister", die sie nicht mehr loswerden sollte.

Sie fügte sämtliche bislang auf ihrem Handy abgespeicherten Rufnummern der minderjährigen Austräger_innen und teilweise auch die von deren Eltern der Chatgruppe hinzu. Zu ihrer Begeisterung wuchs die Gruppe so schnell an, dass eine Gruppengröße von mehreren hundert Personen zustande kam. Die nicht homogene Gruppe bestand aus überregionalen Austräger_innen, die sich persönlich weder kannten noch bislang untereinander Kontakt hatten. Was die Administratorin vermutlich unterschätzte, war die Eigendynamik und Wucht, die aus einer derartigen Chatgruppe entstehen kann. Schnell verselbständigte sich die Gruppe mit Unterhaltungen und gegenseitigen Kontaktanfragen, berufliche Belange spielten keine Rolle mehr. Ungehindert konnten Bilder und Beiträge jedweder Art in den Gruppenchat eingestellt werden. Als die Vorgesetzte sich nicht mehr in der Lage sah, die Gruppe eigens zu bändigen, „verabschiedete" sie sich aus dem Gruppen-Chat und gab damit auch noch die Administratorenrechte auf. Damit waren die gerufenen Geister „herrenlos" und keine Grenzen mehr gesetzt, sodass es auch zur sexuellen Belästigung einer minderjährigen Person kam, was zur Anzeige bei der Polizei gelangte. Der Vorgesetzten blieb nichts anderes übrig, als die technische Abteilung ihrer Firma zu alarmieren, um wieder Herrin über die Gruppe zu werden und sich die Administrationsrechte zurückzuholen. Die Gruppe wurde nach Aussage der Firmenleitung geschlossen.

Die Handlung der Mitarbeiterin ist – trotz der Gesamtumstände – gem. §§ 30 Abs. 1 Nr. 1, 130 Abs. 1 OWiG dem Unternehmen vollumfänglich zurechenbar. Unstrittig lag von Seiten der Teilnehmenden keine Einwilligung i. S. Art. 6 Abs. 1 Buchst. a) DS-GVO oder berechtigtes Interesse zur Verarbeitung i. S. Art. 6 Abs. 1 Bucht. f) DS-GVO der Beschäftigtendaten für diesen Zweck vor.

Mit der Errichtung der Chatgruppe wurden für einen erheblichen Zeitraum die Beschäftigtendaten und die Daten Dritter im Chat offen an einem ungeeigneten und für jeden Zugangsberechtigten öffentlichen Ort verfügbar, ohne angemessene Sicherheits- und Schutzvorkehrungen i.S Art. 32 DS-GVO für die personenbezogenen Daten zu treffen.

Das Unternehmen ließ als verantwortliche Stelle für die Datenverarbeitung außer Acht, dass auf diese Weise personenbezogene Daten der Chatteilnehmenden, wie Profilbilder, Vorname und Namen, Statusberichte etc., die den anderen Teilnehmenden bislang nicht bekannt waren, nun chatintern öffentlich wurden und bei den anderen Mitgliedern der Gruppe auf deren Endgeräten gespeichert werden konnten. Weiter bleib unberücksichtigt, dass die hochgeladenen Fotos – z. B. durch individuelle Backups – gespeichert werden konnten, ohne dass die Betroffenen einen Einfluss auf die weitere Verwendung der Daten durch den Dienst gehabt hätten. Das Unternehmen als verantwortliche Stelle ergriff für die Datenverarbeitung keine Maßnahmen zur Sicherung der Daten bei den Chatteilnehmenden oder beim Messengerdienst.

Auch wurden keine geeigneten Vorkehrungen zur Datensicherheit für den Prozess der Gruppenberechtigung und deren Administratoren getroffen. Die betriebliche Nutzung des weltweit operierenden Messengerdienstes zur Koordination und Steuerung der Austräger_innen mit einer Gruppe von mehreren hundert Personen stellt einen Verstoß gegen Art. 5 Abs. 1 Buchst. f) i.V.m. Art. 32 DS-GVO dar. Personenbezogene Daten der Chatteilnehmenden wurden allen anderen Teilnehmenden offengelegt, ohne dass irgendwelche Sicherheitsmaßnahmen zum Schutz der Daten bei den Empfängern oder dem Messenger-Dienstleister ergriffen wurden. Verstoßen wurde damit gegen die Pflicht zum Schutz und zur Integrität von personenbezogenen Daten.

Wir gehen davon aus, dass wir demnächst das Verfahren mit der Verhängung eines Bußgelds abschließen.

Bußgeldstelle Digitale Dienste

Was sich zunächst nach einer süßen Leckerei anhört, der kaum jemand wiederstehen kann, stellt sich in Zeiten der Digitalisierung als eine Speicherung einer Information auf einem Endgerät – häufig ohne Kenntnis der Nutzenden – dar, was diesen überhaupt nicht schmeckt. Wir sprechen hier also über Cookies.

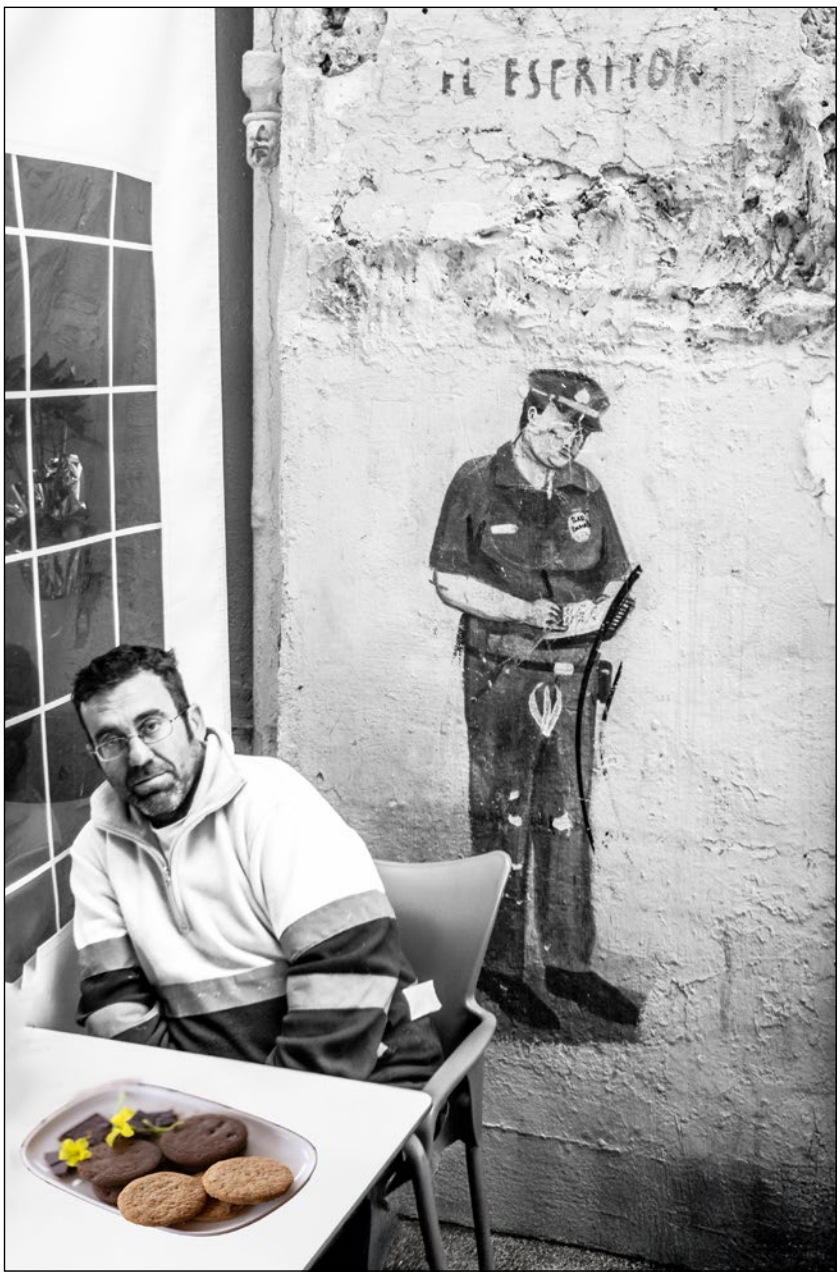
Cookies – lecker?

Informationen werden häufig ohne Einwilligung und ohne jegliche Rechtsgrundlage auf Endgeräten gespeichert. Im Anschluss werden teilweise die so erlangten personenbezogenen Daten an Dritte weitergeleitet, was ggf. einen Verstoß gegen die DS-GVO darstellt. Das ist weder lecker, noch datenschutzkonform.

Am 1. Dezember 2021 trat das Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) in Kraft, welches die Datenschutzregelungen des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) zusammenführen sollte. Am 13. Mai 2024 wurde das TDDSG in „Telekommunikation-Digitale-Dienste-Gesetz (TDDDG) umbenannt, um das deutsche Recht an den Digital Service Act (DSA) anzupassen.

Seit dem 10. Dezember 2022 ist der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden- Württemberg für Verstöße gegen die in § 28 Abs. 1 Nr. 10, Nr. 11 und Nr. 13 TDDDG normierten Vorschriften zuständig (soweit nicht die Bundesbeauftragte zuständig ist).

Bei Verstößen, die gemäß § 28 TDDDG mit einem Bußgeld geahndet werden sollen, gilt das Ordnungs-



Wir würden auch lieber Cookies essen, statt durch sie im Netz verfolgt zu werden.

widrigkeitengesetz (OWiG). Gemäß § 46 OWiG findet die Strafprozessordnung (StPO) entsprechende Anwendung. Die Bußgeldstelle Digitale Dienste hat somit (mit Ausnahmen) dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Die Bußgeldstelle kann dementsprechend unter anderem Durchsuchungs-und Beschlagnahmebeschlüsse erwirken und vollziehen (ggf. auch mit Amtshilfe der Polizei) und Zeugen vernehmen.

In Folge der Übertragung der Zuständigkeit für die in § 28 Abs.1 Nr.10, Nr.11, Nr.13 TDDDG genannten Verstöße werden diese Bußgeldverfahren seit dem 1. August 2024 von dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit durch die hierfür neu eingerichtete Bußgeldstelle Digitale Dienste, welche auch für die Folgeverstöße gegen die DS-GVO zuständig ist, bearbeitet.

An diesem „Plätzchen“ in Baden-Württemberg werden Verstöße gegen das TDDDG und die DS-GVO künftig sanktioniert, um Cookies wieder genießbar zu machen (mehr zu Technisch-organisatorischem Datenschutz s. S. 144 ff.).

Statistische Übersicht

Zeitraum jeweils vom 1. Januar – 31. Dezember

	2017	2018	2019	2020	2021	2022	2023	2024
Beschwerden	3058	3902	3757	4782	4708	3796	3817	4034
Kontrollen	55	13	111	31	10	33	71	54
Beratungen[1]	1786	4440	3842	3285	2206	1935	1682	1360
Anmeldungen Bildungs- und Beratungszentrum BIDIB				785	2016	3255	3732	4470
Datenpannen	121	900	2030	2321	3136	2747	2913	3559
Bußgeldverfahren (eingeleitet)		138	233	174	136	213	185	243
Beteiligung an Gesetzgebungsverfahren[2]								92

1 ohne telefonische Beratung
2 Norm- und Gesetzgebungsverfahren sowie Verordnungen und Verwaltungsvorschriften (vgl. dazu auch S. 43 ff.)

Bild: kwasibanane

Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Baden-Württemberg

Der Landesbeauftragte
für Datenschutz und
Informationsfreiheit
Baden-Württemberg

Covergestaltung: kwasibanane