Ausgabe 01/2024

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

mastodon.social/@bvd@privacyofficers.social

linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD e.V.
DATENSCHUTZ GESTALTEN

BvD-Veranstaltungen

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

09.04.2024	**Webinar – DIN EN ISO 19011 als Leitfaden für interne Datenschutzaudits**
10./11.04.2024	**Online-Seminar: Office 365 – Möglichkeiten und Risiken der Software**
18.04.2024	**Webinar – „EU-ACTionism: Digital Governance Act“**
24.04.2024	**Online-Seminar: KI für KMU**
30.04.2024	**Webinar – Clear Web, Deep Web, Dark Web: Eine Reise in die Untiefen des Internets. Wir gehen mit dem TOR-Browser auf U-Boot fahrt**
02.05.2024	**Webinar – „EU-ACTionism: AI Act“**
07.05.2024	**Online-Seminar: Drittlandtransfer - Internationaler Datenschutz**
27.05.2024	**Sonder-Seminar: Sonderfälle im Beschäftigtendatenschutz**
27.05.2024	**Sonder-Seminar: Videoüberwachung: Was geht, was geht nicht?**
28. – 29.05.2024	**BvD-Verbandstage 2024 in Berlin**
04.06.2024	**Online-Seminar: Datenschutzaudit und Datenschutzkontrolle**
06.06.2024	**Webinar – „EU-ACTionism: NIS 2-Richtlinie und Cyber Resilience Act“**
25.06.2024	**3. Datenschutztag Hessen & Rheinland-Pfalz in Frankfurt/Main**
27.06.2024	**Webinar – Privacy Litigation aus der Sicht des DSB: Einordnung und Umgang mit Schadensersatzansprüchen**
17.09.2024	**Webinar – Clear Web, Deep Web, Dark Web: Eine Reise in die Untiefen des Internets. Wir gehen mit dem TOR-Browser auf U-Boot fahrt**

JETZT ANMELDEN:
bvdnet.de/termine

Liebe Leserinnen und Leser,

gerade war die letzte BvD-News 2023 erschienen, da legte der EuGH beim Thema Datenschutz noch einmal richtig los: Im Dezember traf er gleich eine ganze Reihe von Entscheidungen. Da ging es um Fragen zum Thema Bußgelder, es ging um Scoring und Auskunfteien, es ging um Erlaubnistatbestände und um TOM.

Von dieser Entscheidungsflut und ihren Auswirkungen auf die praktische Seite des Datenschutzes ist unsere neue Ausgabe geprägt. Wir hoffen, dass wir damit an der einen oder anderen Stelle Klarheit zur Auslegung der Urteile bringen können. Und wir sind weiterhin gespannt: Denn der EuGH hat sich nicht erst seit den Schrems-Urteilen zum Fachgericht für Datenschutz-Fragen entwickelt. Wir dürften also noch weitere Entscheidungen erwarten, von denen Sie hier auch in Zukunft lesen werden.

Um so wichtiger ist es, dass die EU-Kommission im sechsten Jahr nach dem Start der DSGVO eine Evaluation unternimmt, die diesen Namen verdient. Die Wahrscheinlichkeit ist allerdings eher gering, dass diese Hoffnung erfüllt wird – wie auch schon unsere politische Diskussionsveranstaltung im September 2023 zu diesem Thema schlussfolgerte. Wir als BvD und auch unser europäischer Dachverband EFDPO haben dennoch Positionspapiere veröffentlicht, die Sie auf den jeweiligen Websites (bvdnet.de und efdpo.eu) finden.

Eine echte Evaluation wäre auch deshalb lohnenswert, weil der europäische Gesetzgeber dann nicht die Auslegungskompetenz in Sachen Datenschutz dem EuGH überlässt. Doch nach wie vor warten wir auf die bereits im vergangenen Sommer angekündigte „Enforcement"-Verordnung, die Bußgeldverfahren in den EU-Mitgliedsstaaten vereinheitlichen und vereinfachen will. Eigentlich wollte das EU-Parlament darüber im Februar befinden.

Etwas weiter sind wir beim Thema AI Act, über dessen aktuellen Stand Prof. Dr. Thomas Wilmer schreibt. Auch Rechtsanwältin Nina Diercks nimmt bei ihrem Schwerpunktthema KI beim Personal-Recruiting Bezug auf die jüngsten Änderungen an dem Entwurf, Thea Mustać reflektiert über die Frage, was affektive KI eigentlich ist.

Außerdem hat die Schweiz ein neues Datenschutzrecht. Was dies für Datenschutzbeauftragte in Deutschland bedeutet, fasst David Vasella für uns zusammen. Und wir beschäftigen uns mit der Frage ob Anonymisierung und Pseudonymisierung tatsächlich aus datenschutzrechtlicher Sicht eine Lösung darstellen können.

Insbesondere für behördliche Datenschutzbeauftragte stellt sich die Frage nach dem Stand der Verwaltungsdigitalisierung. Katja Horlbeck vom Hessischen Datenschutzbeauftragten bringt hier Licht ins Dickicht.

Aber nicht alles beim Thema Datenschutz muss komplex und kompliziert sein. Die drei Nominierten für die diesjährige DAME-Preisverleihung zeigen dies wieder eindrücklich. Datenschutz kann man auch einfach erklären, lustig umsetzen und gezielt für Kinder und Jugendliche in ihrer Sprache und für ihre Fragen aufbereiten. Wer in diesem Jahr ins Rennen um unsere DAME geht, das erfahren Sie ebenfalls in dieser Ausgabe.

Ich wünsche Ihnen eine erhellende und vergnügliche Lektüre zugleich.

Ihr

T. Spaeing

Thomas Spaeing
BvD-Vorstandsvorsitzender

INHALTSVERZEICHNIS

IMPRESSUM

BvD-News

Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Herausgeber

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.
Budapester Straße 31
10787 Berlin
Tel: 030 26 36 77 60
Fax: 030 26 36 77 63
E-Mail: bvd-gs@bvdnet.de
Internet: bvdnet.de
mastodon.social/@bvd@privacyofficers.social
linkedin.com/company/berufsverband-der-datenschutzbeauftragten
bvdnet.de/feed/
bvdnet.de/themen/bvd-blog/

Redaktion

Christina Denz (chd)
V.i.S.d.P.: Thomas Spaeing
bvd-news@bvdnet.de

Fotos (sofern nicht anderweitig ausgewiesen)

Adobe Stock, 123RF Foto
Foto S. 59 Jason Goodman auf Unsplash.com
Foto S. 60 Fotolia

Lektorat

Frank Spaeing, Regina Mühlich

Anzeigen

Christina Denz

Kooperationen

Malaika Ngoy, Karsten Füllhaase (bvd-gs@bvdnet.de)

Satz, Layout & Produktion

Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
tpmarketing.de

ISSN: 2194-1025

Erscheinungsweise: 3 x jährlich, Druckauflage 4.000 Exemplare (Unsere Mediadaten erhalten Sie unter bvdnet.de/Publikationen oder von unserer Geschäftsstelle per E-Mail an bvd-gs@bvdnet.de) Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

IM FOKUS

DATENSCHUTZRECHT

DATENSCHUTZPRAXIS

Wollen Sie aus einem Artikel in der BvD-News zitieren?
Unser Zitiervorschlag:
Autor(en), BvD-News Ausgabe x/20xx, Seite xx

Scannen Sie den QR-Code und gelangen Sie zu allen Ausgaben der BvD-News ab 1997

PROF. DR. THOMAS WILMER

KI-VERORDNUNG: DATENSCHUTZRECHTLICHE HERAUSFORDERUNGEN

Nachdem die EU die KI-Verordnung auf den Weg gebracht hat[1], stellt sich die Frage nach den Konsequenzen für die Zukunft des Datenschutzes beim Einsatz Künstlicher Intelligenz. Begrüßenswert ist die Tatsache der Einheitlichkeit der Regelung in Europa, nachdem unter anderem die DSK eine klare Verantwortlichkeit für Hersteller und Betreiber eingefordert hatte[2]. Die nach dem Trilog absehbare Endfassung erhält einige Vorgaben, die sowohl neue Rechtsgrundlagen für die Datenverarbeitung, vor allem aber auch neue Dokumentationspflichten betreffen[3]. Mit dem Anwendungsbeginn der KI-VO ist Mitte/Ende 2026 zu rechnen.

1. Regelungsgehalt der KI-Verordnung

Zweck der KI-Verordnung (im Folgenden „KI-VO-E") nach deren ErwGr. 1 ist es, einen einheitlichen Rechtsrahmen insbesondere für die Entwicklung, Vermarktung und Verwendung künstlicher Intelligenz im Einklang mit den Werten der Union festzulegen, um unter Anderem ein hohes Schutzniveau der Gesundheit, der Sicherheit und der Grundrechte sicherzustellen. Gewährleistet werden soll ebenfalls der grenzüberschreitende freie Verkehr KI-gestützter Waren und Dienstleistungen. Nach ErwGr. 5 soll dadurch das Ziel der Union umgesetzt werden, bei der Entwicklung einer „sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz" weltweit eine Führungsrolle einzunehmen. Die wesentlichen Regelungsinhalte der geplanten KI-Verordnung der EU beinhalten zum Einen die Einführung von Risikoklassen, bei welchen KI-Anwendungen basierend auf ihrem potenziellen Schaden und ihrer Gefährlichkeit einer

[1] Stand 15.02.2024 nach Verabschiedung des Entwurfs durch den Ausschuss der Ständigen Vertreter (AStV), Ergebnisüberblick zum Trilog bei Bomhard/Siglmüller, RDi 2024, 45. Nach der Zustimmung des EU-Parlaments am 13. März erstellt der Autor ein Dokument mit möglichen Änderungen in der finalen Version, sobald sie vorliegt, auf chatgpt-recht.de

[2] DSK, Pressemitteilung vom 23.11.2023, https://www.datenschutzkonferenz-online.de/media/pm/23-11-29_DSK-Pressemitteilung_KI-Regulierung.pdf, siehe auch Initiative „AI Act verabschieden", https://www.ai-act-verabschieden.de/

[3] Stand zu Redaktionsschluss: https://fbgw.h-da.de/fileadmin/user_upload/AIAct_final_four-column21012024.pdf

Einstufung unterzogen werden. Hochriskante KI-Systeme werden mit Auflagen hinsichtlich der Risikobegrenzung und der Entwicklungsqualität belegt. Daneben enthält die KI-VO ein Verbot bestimmter Anwendungen von Künstlicher Intelligenz, die als besonders gefährlich oder ethisch bedenklich betrachtet werden.

Weiterhin sind auch Vorgaben für Transparenz und Dokumentationspflichten enthalten: Entwickler und Anbieter von KI-Systemen werden verpflichtet, transparent über die Funktionsweise ihrer Systeme zu informieren. Dies kann auch die Dokumentation von Algorithmen und Trainingsdaten umfassen. Die KI-VO enthält schließlich neue Rechtsgrundlagen zur Verarbeitung personenbezogener Daten zur KI-Qualitätssicherung.

2. Datenschutzrechtliche Herausforderungen der KI

KI wird im KI-VO-E in Art. 3 Nr. 1 wie folgt definiert: „Ein KI-System ist ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach seiner Einführung eine Anpassungsfähigkeit aufweist, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können." KI ist somit eine Art Vorhersagetechnik auf basierenden Erfahrungen und Trainingsdaten. Der Erwägungsgrund 45a KI-VO-E nennt als Maßnahmen zur Wahrung des Datenschutzes die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen des Art. 25 DSGVO, wenn die Verarbeitung von Daten erhebliche Risiken für die Grundrechte natürlicher Personen birgt. Als zugehörige technische und organisatorische Maßnahmen werden neben der Anonymisierung und Verschlüsselung auch der „Einsatz zunehmend verfügbarer Technik" genannt, „die es ermöglicht, Algorithmen direkt am Ort der Datenerzeugung einzusetzen und wertvolle Erkenntnisse zu gewinnen, ohne dass die Daten zwischen den Parteien übertragen beziehungsweise die Rohdaten oder strukturierten Daten selbst unnötig kopiert werden."
Fraglich ist, ob sich in der Umsetzung der Regulierung die Konflikte zwischen KI-Funktionalitäten und Datenschutzbedürfnissen befriedigend auflösen lassen werden.

Damit KI funktioniert, muss sie über eine möglichst umfassende, korrekte und aktuelle Datenbasis verfügen, welche sie auswerten und inhaltlich verknüpfen kann. Insofern enthält die KI-Anwendung auch immer einen „Big Data"-Aspekt. KI und Datenschutz befinden sich damit in einem Spannungsverhältnis, soweit KI personenbezogene Daten im Sinne der Art. 4 Nr. 1 DSGVO verarbeitet. Dies ist regelmäßig der Fall, da aus dem Internet und aus Nutzereingaben ausgelesene beziehungsweise gespeicherte Daten in das KI-Modell einfließen und für die Ergebnisausgabe weiterverarbeitet werden[4].

Im Einsatz in Apps oder auf Webseiten kann KI in verschiedenen Bereichen personenbezogene Daten einsetzen. Zum einen können personenbezogene Daten in Form von Namen, namensbezogenen Informationen, Bildern und biometrischen Daten in die Trainingsdatenbasis Einzug gehalten haben. Zum anderen können Nutzer durch die Eingabe von Anfragen (sog. Prompts) Daten mit Personenbezug in die KI einspeisen, welche dann möglicherweise der Trainingsdatenbank hinzugefügt werden. In jüngster Zeit wird aufgrund der zunehmenden Fehlerhaftigkeit von KI-Ergebnissen, welche auf allgemeinen Internetauswertungen basieren[5], ein Aufbau nutzerbezogener Trainingsdatenbanken („Gedächtnis") angeboten[6].

Und schließlich kann die Ausgabe von Daten wieder mit Personenbezug erfolgen, etwa wenn ein Prompt eine Darstellung der Biografie einer natürlichen Person angefordert hat. Soweit Trainingsdaten nach und nach in das KI-System überführt werden und bei ihrer Kombination ein Personenbezug sukzessive ermöglicht wird, muss dies bei entsprechenden technisch-organisatorischen Maßnahmen noch nicht dazu führen, dass automatisch ein Personenbezug bejaht wird, wenn das KI-System – unter anderem durch Datentrennungsmaßnahmen – nicht auf die Herstellung dieser Bezüge ausgerichtet ist.[7] Der Aufbau nutzerbezogener „Gedächtnisse" wird dies jedoch grundlegend ändern, da sowohl eine nutzerbezogene Verknüpfung der Nutzung abrufbar ist als auch eine Agglomeration der Daten und Kombination mit weiteren Nutzerdaten – etwa aus anderen Anwendungen des gleichen KI-Anbieters, bei welchem der Nutzer registriert ist. Nach der Eröffnung des ChatGPT-Stores können darüber hinaus weitere Akteure ChatGPT in ihre Anwendungen integrieren und dort Nutzerdaten aggregieren[8].

[4] Zur entsprechenden Forderung nach klaren Datenschutzregelungen auch Bomhard/Siglmüller, RDi 2024, 45, 55.

[5] Kathun, Brown, Reliability Check: An Analysis of GPT-3's Response to Sensitive Topics and Prompt Wording, Preprint, https://arxiv.org/pdf/2306.06199.pdf.

[6] OpenAI-Meldung vom 13.2.2024, Memory and new controls for ChatGPT, https://openai.com/blog/memory-and-new-controls-for-chatgpt. Welche Nachteile nutzerbezogene Gedächtnisse haben können, zeigt der Fall des DPD-eigenen Chatbots, welcher auf Nutzeranfrage über den eigenen Paketdienst zu fluchen begann, vermutlich aufgrund des Zugriffs auf DPD-interne Chats der Beschäftigten („DPD is useless", „DPD is the worst delivery firm in the world"), https://twitter.com/ashbeauchamp/status/1748034519104450874

[7] Ashkar, ZD 2023, 523, 524f.

[8] https://openai.com/blog/introducing-the-gpt-store

Verantwortliche für die Datenverarbeitung sind die Betreiber der KI und einsatzabhängig die Nutzer – gegebenenfalls in gemeinsamer Verantwortlichkeit nach Art. 26 DSGVO[9]. Die KI-Betreiber werden in aller Regel eigene Zwecke mit der Bereitstellung der KI verfolgen, indem diese durch die Nutzereingaben weiter lernt und die Datenbasis verbreitert. Soweit daher aus den Prompts Daten für das Training der KI gewonnen werden, wird eine Auftragsverarbeitung nach Art. 28 DSGVO als datenschutzrechtliche Einordnung ausscheiden. Vor diesem Hintergrund sind auch Aussagen von Microsoft zu betrachten, nach denen beim Einsatz vom MS Copilot keine Nutzereingaben zum KI-Einsatz verwendet werden und ein „AI Safety Mechanism" entsprechende Datenflüsse unterbindet[10].

Im Hinblick auf die Funktionsweise der KI können Konflikte mit den Grundsätzen des Datenschutzes nach Art. 5 DGSVO auftreten, etwa dem Grundsatz der Transparenz und dem Grundsatz von Treu und Glauben, welcher u.a. ein Diskriminierungsverbot enthält[11], das aufgrund der Verpflichtung zur rechtmäßigen Verarbeitung auch Verstöße gegen das AGG umfasst. Dementsprechend sind diskriminierende – und bereits nicht nachvollziehbare Entscheidungswege – von KI bereits datenschutzrechtlich problematisch, ohne dass es auf die entsprechenden Vorgaben der KI-VO ankommt. Nach Art. 5 Abs. 1 lit d) DSGVO haben Daten darüber hinaus sachlich richtig und erforderlichenfalls auf dem neuesten Stand zu sein; dies erfordert eine Kontrolle der Daten des Input und des Outputs der KI, mithin eine Qualitätskontrolle der Trainingsdaten und ihrer Quellen sowie der Ergebnisse der Verarbeitung durch die KI.[12] Insbesondere das Erfinden und „Halluzinieren" von Ergebnissen[13] ist dementsprechend kritisch zu betrachten. Weiterhin erfordert Art. 25 DSGVO die bereits angesprochene Konzeption von KI-Systemen bei der Verarbeitung personenbezogener Daten nach den Grundsätzen von „Privacy by default" und „Privacy by design".
Die Datenschutzaufsichten haben vielfach zu Grundsätzen des Datenschutzes beim KI-Einsatz Stellung genommen. Die baden-württembergische Aufsicht hat ein Papier zu Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz veröffentlicht[14], die Hamburger Aufsicht eine Checkliste zum Einsatz LLM basierter Chatbots[15], zuletzt die bayrische Aufsicht eine Checkliste „Datenschutzkonforme Künstliche Intelligenz mit Prüfkriterien nach DS-GVO[16]."

3. Beispiel Microsoft CoPilot

Ein Beispiel für die umfassende Verknüpfung von Daten aus Nutzereingaben, Nutzerdatenbeständen und ChatGPT ist der neu in Office integrierte Microsoft „Copilot". Copilot basiert auf ChatGPT, wird in jeder Office-Anwendung – einschließlich Teams – integriert sein und sowohl auf Datenquellen aus dem Internet über Bing, als auch auf alle in Microsoft Graph gespeicherte Unternehmensdaten zugreifen können. Copilot kann genutzt werden, um Videokonferenzen oder E-Mailposteingänge zu analysieren und zusammenzufassen[17]. Da der Copilot nicht in rechtlichen Kategorien, sondern technischen Verfügbarkeiten „denkt", ist eine umfassende Verknüpfung aller vorhandenen Daten auf Nutzeranfrage hin möglich („Wer hat zu diesem Thema eine Mail verfasst?", „Wer sollte an einer Projektbesprechung teilnehmen", aber auch „Wer hat die angeordnete Kundenmail noch nicht abgesendet?"). Hier stellen sich komplexe Aufgaben der Eingrenzung des Anwendungsbereichs, des Umgangs mit Privatnutzungen in Office, der Zulässigkeit automatisierter Entscheidungen nach Art. 22 DSGVO und auch der arbeitsrechtlichen Rahmenbedingungen[18]. Copilot wird damit vermutlich der verbreitetste Fall der Integration von

[9] Conrad, K&R 2018, 741, 743. vgl. zu rechtspolitischen Fragen Hermonies, in: Schreiber/Ohly (Hrsg.), KI:Text. Diskurse über Textgeneratoren, 2023, S. 329ff.

[10] https://learn.microsoft.com/de-de/microsoft-365-copilot/microsoft-365-copilot-privacy

[11] Baumgartner/Brunnbauer/Cross, MMR 2023, 543, unter Verweis auf ErwGr. 71 S. 6, 75 und 85 S. 1 DSGVO.

[12] Baumgartner/Brunnbauer/Cross, MMR 2023, 543, 546.

[13] Berz/Engel/Hacker, ZUM 2023, 586, 587 m.w.N.; Beispiele zu Falschergebnissen bei Wilmer, K&R 2023, 233, 237f.; Wilmer, K&R 2023, 385, 390.

[14] „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz. Wann und wie dürfen personenbezogene Daten für das Training und die Anwendung von Künstlicher Intelligenz verarbeitet werden?", Diskussionspapier. Version 1.0 vom 07.11.2023, https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/

[15] Checkliste vom 13.11.2023, https://datenschutz-hamburg.de/news/checkliste-zum-einsatz-llm-basierter-chatbot

[16] Checkliste vom 24.1.2024, https://www.lda.bayern.de/media/ki_checkliste.pdf

[17] Anwendungsbeispiele unter https://fbgw.h-da.de/fileadmin/Fachbereich_GW/3.Forschung/3.2Forschungsprojekte/Rechtsfragen_Copilot_Plattform_Wilmer.pdf

[18] Checkliste zur Copilot-Einführung abrufbar unter https://fbgw.h-da.de/forschung/chatgpt-dall-e-co/faq-copilot

ChatGPT und KI mit allgemeinem Verwendungszweck (sog. GPAI[19]) in Unternehmensanwendungen darstellen. Ob allerdings – wie Microsoft es darstellt – die Nutzerangaben nicht an Microsoft oder ChatGPT zurückfließen (sog. „AI Safety Mechanism“[20]), kann nicht wirklich kontrolliert werden. Fände ein solcher Rückfluss zu eigenen Trainingszwecken von Microsoft statt, würde dies allerdings das Modell einer Auftragsverarbeitung durch Microsoft nach Art. 28 DSGVO in Frage stellen. Microsoft Copilot stellt daher umfassende Anforderungen an die datenschutzrechtliche Einordnung und die vorab erforderliche Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.

4. Datenschutzregelungen in der KI-Verordnung

Die KI-VO enthält neben Regulierungsvorgaben auch neue Erlaubnistatbestände für die Verarbeitung personenbezogener Daten. Nach Art. 10 Abs. 5 S. 1 KI-VO-E dürfen die Anbieter von Hockrisiko-KI-Systemen ausnahmsweise besondere Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 der Verordnung (EU) 2016/679, Artikel 10 der Richtlinie (EU) 2016/680 und Artikel 10 Absatz 1 der Verordnung (EU) 2018/1725 verarbeiten, soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist. Hierbei müssen sie jedoch nach Art. 10 Abs. 5 S. 2 KI-VO-E angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen, welche kumulativ folgende Voraussetzungen erfüllen müssen:

(a) Die Erkennung und Korrektur von Verzerrungen kann nicht durch die Verarbeitung anderer Daten, einschließlich synthetischer oder anonymisierter Daten, wirksam durchgeführt werden;
(b) für die besonderen Kategorien personenbezogener Daten, die für diese Zwecke verarbeitet werden, gelten technische Beschränkungen für die Weiterverwendung der personenbezogenen Daten und dem Stand der Technik entsprechende Sicherheits- und Datenschutzmaßnahmen, einschließlich Pseudonymisierung;
(c) die besonderen Kategorien personenbezogener Daten, die für diese Zwecke verarbeitet werden, sind Gegenstand von Maßnahmen, die gewährleisten, dass die verarbeiteten personenbezogenen Daten gesichert und geschützt werden und geeigneten Garantien unterliegen, einschließlich strenger Kontrollen und der Dokumentation des Zugangs, um Missbrauch zu vermeiden und sicherzustellen, dass nur befugte Personen mit angemessenen Vertraulichkeitsverpflichtungen Zugang zu diesen personenbezogenen Daten haben;

[20] Siehe Nachweise zu Microsoftangeben unter https://fbgw.h-da.de/fileadmin/Fachbereich_GW/3.Forschung/3.2Forschungsprojekte/Rechtsfragen_Copilot_Plattform_Wilmer.pdf

[19] „General Purpose AI“, unterschieden im Art. 52a KI-VO-E nach GPAI models und GPAI models with systemic risks. Bei letzteren bleibt abzuwarten, welche Konsequenzen das Schufa-Urteil des EuGH auf GPAI haben wird, welche Entscheidungen im Sinne des Art. 22 DSGVO treffen soll, vgl. Buck-Heeb, EuZW 2024, 49.

(d) die besonderen Kategorien personenbezogener Daten, die für diese Zwecke verarbeitet werden, dürfen nicht an andere Parteien übermittelt, weitergegeben oder anderweitig zugänglich gemacht werden.

Diese Einschränkungen wurden in den Trilogverhandlungen zuletzt eingebracht und durch Erwägungsgrund 72a begleitet, welcher vorsieht, dass festgestellte erhebliche Risiken für die Sicherheit, die Gesundheit und die Grundrechte, die bei der Entwicklung und Erprobung im Sandkasten auftreten können, angemessen zu mindern sind.

Zu den Verpflichtungen der Betreiber von Hochrisiko-KI-Systemen nach Art. 29 Abs. 6 gehört es, dass die gemäß Artikel 13 KI-VO-E bereitgestellten Informationen zur Information über das KI-System auch verwendet werden, um gegebenenfalls ihrer Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung gemäß Artikel 35 DSGVO nachzukommen.

Im Hinblick auf den umstrittenen Biometrie-Einsatz setzt Art. 29 Abs. 6a KI-VO-E voraus, dass unbeschadet der Richtlinie (EU) 2016/680 der Betreiber eines KI-Systems für die biometrische Identifizierung im Nachhinein im Rahmen von Ermittlungen zur gezielten Durchsuchung einer Person, die einer Straftat überführt oder verdächtigt wird, vor oder unverzüglich und spätestens innerhalb von 48 Stunden eine Genehmigung für die Verwendung des Systems bei einer Justizbehörde oder einer Verwaltungsbehörde beantragt, deren Entscheidung verbindlich ist und gerichtlich überprüft werden kann, es sei denn, das System wird für die erste Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und überprüfbarer Tatsachen, die unmittelbar mit der Straftat in Verbindung stehen, verwendet.

Art. 29a KI-VO-E sieht die Verpflichtung zu einer umfassenden grundrechtlichen Folgenabschätzung für hochriskante KI-Systeme vor, welche unter anderem eine klare Darstellung des beabsichtigten Verwendungszwecks und des geplanten geografischen und zeitlichen Anwendungsbereichs des Systems sowie spezifische Schadensrisiken, die sich auf marginalisierte Personen oder schutzbedürftige Gruppen auswirken könnten, umfassen muss. Erforderlich ist weiterhin ein ausführlicher Plan, wie das erkannte Schadensrisiko sowie die negativen Auswirkungen auf die Grundrechte gemindert werden sollen. Nach Anhang VIII Abschnitt B sind in der Folge zu den KI-Hochrisiko-Systemen unter anderem KI-Systemen eine Zusammenfassung der Ergebnisse der gemäß Artikel 29a KI-VO-E durchgeführten Folgenabschätzung für die Grundrechte und eine Zusammenfassung der durchgeführten Datenschutz-Folgenabschätzung bekannt zu machen und aktuell zu halten.Weitere Regelungen betreffen die in Art. 53 KI-VO-E vorgesehenen KI-Reallabore, welche KMU bei der Erfüllung regulatorischer Pflichten unterstützen sollen. Art. 53 Abs. 2 KI-VO-E sieht vor, dass die Mitgliedstaaten dafür sorgen, dass „KI-Sandboxen" unter Beteiligung der zuständigen Aufsichten eingerichtet werden. Diese sollen für ein kontrolliertes Umfeld sorgen, das Innovation fördert und Entwicklung, Training, Prüfung und Validierung von innovativen KI Systemen für eine begrenzte Zeit vor ihrem Inverkehrbringen oder Inbetriebnahme gemäß einem spezifischen „Sandboxplan", der zwischen den potenziellen Anbietern und der zuständigen Behörde vereinbart wurde, ermöglicht. Solche Sandboxes empfehlen sich generell auch für die datenschutzrechtlich gebotene Einrichtung von Anwendungsszenarien, um mögliche KI-Einsatz-Risiken für die Betroffenen zu erkennen und diesen rechtzeitig vorzubeugen.

FAZIT

Insbesondere beim Einsatz komplexer KI-Systeme wie GPAI wird neben der Risikoeinstufung die Kontrolle der Datenschutzvorgaben zu erheblichen Herausforderungen führen. Dementsprechend sollte rechtzeitig vor dem Einsatz geplant werden, inwiefern auch innerhalb der verantwortlichen Stelle eine „Sandbox" eingerichtet wird, in welcher die Einsatzparameter und Zugriffsoptionen auf personenbezogene Daten geprüft werden können, bevor ein Datenabfluss an die KI-Anbieter – auch im Testbetrieb – erfolgen kann.

Über den Autor

Prof. Dr. Thomas Wilmer
ist geschäftsführender Direktor des Instituts für Informationsrecht an der Hochschule Darmstadt und lehrt in der Fachanwaltsausbildung für Informationstechnologierecht. Außerdem ist er Datenschutzbeauftragter der Hochschule Darmstadt und betreibt die Informationsseite chatgpt-recht.de.

Jetzt 3 Monate ZD kostenlos testen.

ZD – Zeitschrift für Datenschutz

14. Jahrgang. 2024. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 343,–
Vorzugspreis für BvD-Mitglieder, für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 269,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 18,– jährlich.

beck-shop.de/go/ZD

Die große Zeitschrift zum Datenschutz

Die ZD informiert umfassend über die relevanten datenschutzrechtlichen Aspekte aus allen Rechtsgebieten und begleitet die nationale sowie internationale Gesetzgebung und Diskussion um den Datenschutz. Im Mittelpunkt stehen Themen aus der Unternehmenspraxis wie z. B. ▪ Konzerndatenschutz ▪ Beschäftigtendatenschutz ▪ Datenschutz-Folgenabschätzung ▪ Compliance ▪ Kundendatenschutz ▪ Telekommunikation ▪ Soziale Netzwerke ▪ Datentransfer in Drittstaaten ▪ Vorratsdatenspeicherung ▪ Informationsfreiheit ▪ Profiling und Scoring ▪ Tracking.

Geschaffen für die Unternehmenspraxis

Jedes Heft enthält ein Editorial, Aufsätze mit Lösungsvorschlägen, Angaben zur Lesedauer, Abstracts in Deutsch und Englisch, Schlagwortketten, Entscheidungen mit Anmerkungen und aktuelle Meldungen.

Alles inklusive:

- Online-Modul ZDDirekt – vollständiges Online-Archiv ab ZD 1/2011
- 14-täglicher Newsdienst ZD-Aktuell
- Homepage www.zd-beck.de
- Fundstellen-Recherche in beckonline.

3 Hefte gratis

Bestellen Sie das kostenlose Schnupperabo unter www.beck-shop.de/go/ZD.

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812
Folgen Sie uns auf Mehr Infos: ch.beck.de/socialmedia

C.H.BECK

KI IM PERSONAL-WESEN

Was sagt die KI-Verordnung dazu?

Nina Diercks

„KI-Systeme revolutionieren die (Personal-)Arbeit!" so schallt es aus HR-Blogs[1], Fachmagazinen[2] und Leitmedien[3]. Kaum ein Anbieter digitaler HR-Anwendungen kommt noch ohne das Schlagwort "Künstliche Intelligenz" aus. Gleich ob Programmatic Advertiser wie Jobvector, Bewerber- und Personalmanagementsysteme wie Rexx, Workday oder Personio oder Personalentwicklungsplattformen wie Zavvy, Sie alle werben mit KI in ihren Anwendungen.[4] Sei es, dass die Schaltung von Stellenanzeigen „KI-optimiert", das Lebenslauf-Parsing „KI-unterstützt" oder das Personalcontrolling „KI-basiert" erfolgt.

Dazu hat der europäische Gesetzgeber ein Gesetz zur Regelung von künstlicher Intelligenz, die KI-Verordnung, verabschiedet. Die Verordnung enthält unter anderem spezielle Vorschriften für KI-Systeme im HR-Kontext.

Infolgedessen müssen sich Personalverantwortliche sowie (Rechts-)Berater*innen intensiv mit dem Thema KI und der KI-Verordnung auseinandersetzen.

1. Was ist KI?

Alle reden von KI. Doch was ist darunter tatsächlich zu verstehen?

Die nachfolgende Beschreibung der „Künstlichen Intelligenz" ist recht verständlich und ähnelt inhaltlich dem Begriff der KI, wie ihn die KI-Verordnung definiert (siehe dazu weiter unten):

Künstliche Intelligenz ist der Überbegriff für Anwendungen, bei denen Maschinen menschenähnliche Intelligenzleistungen wie Lernen, Urteilen und Problemlösen erbringen. Die Technologie des maschinellen Lernens (ML) – ein Teilgebiet der künstlichen Intelligenz – lehrt Computer aus Daten und Erfahrung zu lernen und Aufgaben immer besser auszuführen. Ausgefeilte Algorithmen können in unstrukturierten Datensätzen wie Bildern, Texten oder gesprochener Sprache Muster erkennen und anhand dieser Entscheidungen selbstständig treffen.[6]

1.1. KI im allgemeinen Sprachgebrauch

Im allgemeinen Sprachgebrauch wird nicht zwischen KI und Machine Learning (ML) unterschieden. Vielmehr wird der Begriff „künstliche Intelligenz" dafür genutzt, einfache bis komplexe Algorithmen zu beschreiben. Dabei wird häufig von schwacher und starker KI gesprochen. Eine schwache KI ist etwa ein Lebenslauf-Parsing, bei dem ein Algorithmus anhand von Faktoren wie einer Schulnote Lebensläufe vorsortiert. Eine starke KI beschreibt dem gegenüber einen

[1] Lilie, Künstliche Intelligenz (KI) in der Personalarbeit, perwiss.de, 15.11.2023, https://kurzelinks.de/u06c.

[2] Bartscher/Nissen, Wie KI den Arbeitsalltag von HR in Zukunft prägt, Haufe Personal, 18.01.2024, https://kurzelinks.de/ok34.

[3] Eckert/Landberg/Pouplier, Kollege KI – Jobkiller oder praktischer Helfer, Video-Beitrag vom 08.07.2023, https://kurzelinks.de/39et

[4] Jobvector, https://kurzelinks.de/gj1u; Rexx, https://kurzelinks.de/tws6; Workday, https://kurzelinks.de/ctzj; Personio, https://kurzelinks.de/uwh7; Zavvy, https://kurzelinks.de/f4ce.

[5] Am 24.01.2024 wurde die im Trilog-Verfahren abgestimmte Fassung der Öffentlichkeit vorgestellt, im Februar haben die Mitgliedstaaten und die beteiligten Parlamentsausschüsse diesem Entwurf zugestimmt.

[6] Schick, Was ist künstliche Intelligenz, SAP News Center, 20.02.2018, https://kurzelinks.de/2209.

weit komplexeren Algorithmus, der etwa die Identifikation von erfolgreichen Mitarbeitern auf Basis von vorliegenden Performance-Daten und unter vorgegebenen Parametern vornimmt. Deutlich wird hier jedoch, dass stets mathematische Algorithmen im Raum stehen. Algorithmen basieren auf Wenn-Dann-Beziehungen und sind von den (durch Menschen) vorgegebenen mathematischen Rechenwegen und die vorhandene Datenbasis beschränkt beziehungsweise von diesen abhängig.

Auch ChatGPT wird im allgemeinen Sprachgebrauch als KI bezeichnet. Dabei handelt es sich um ein Large Language Model. Ein solches LLM errechnet auf einer sehr großen Datenbasis Wahrscheinlichkeiten, welche Wörter statisch am wahrscheinlichsten hinter einem anderen auftaucht. Nach welchen Wörtern ChatGPT dabei zu suchen hat, hängt von der Eingabe, dem Prompt ab. ChatGPT ist also auch nur ein – zugegeben komplexer - Algorithmus, der nach vorgegebenen Rechenwegen Wahrscheinlichkeiten berechnet.

ChatGPT kann selbst aber keine Inhalte erkennen und bewerten und insoweit auch keine Schlussfolgerungen treffen. (Eine andere Frage ist, ob das was ChatGPT, Midjourney & Co am Ende ausgeben nach menschlichem Verständnis „kreativ" ist und in irgendeiner Form rechtlich geschützt sein könnte).

1.2. KI nach der KI-Verordnung

Sehen wir uns nun einmal an, wie Art. 3 Nr. 1 der KI-VO[7] „künstliche Intelligenz Systeme" definiert:

„Ein KI-System ist ein maschinengestütztes System, das so konzipiert ist, dass es mit unterschiedlichem Grad an Autonomie operieren kann und nach seiner Einführung Anpassungsfähigkeit zeigt, und das für explizite oder implizite Ziele aus den Eingaben, die es erhält, ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können."

In Erwägungsgrund 6 (eine Interpretationshilfe des EU-Gesetzgebers zum neuen Gesetz) heißt es unter anderem weiter:

[...] Zu den Techniken, die beim Aufbau eines KI-Systems Inferenzen [logische Schlussfolgerungen] ermöglichen, gehören Ansätze des maschinellen Lernens, die aus Daten lernen, wie bestimmte Ziele erreicht werden können, sowie logik- und wissensbasierte Ansätze, die aus kodiertem Wissen oder einer symbolischen Darstellung der zu lösenden Aufgabe Inferenzen [Schlussfolgerungen] ziehen. Die Fähigkeit eines KI-Systems, Schlüsse zu ziehen, geht über die grundlegende Datenverarbeitung hinaus und ermöglicht Lernen, Schlussfolgerungen oder Modellierung."

Erwägungsgrund 6 enthält auch eine Negativdefinition:

„[...] Der Begriff KI-Systeme [...] sollte nicht für Systeme gelten, die ausschließlich auf von natürlichen Personen festgelegten Regeln zur automatischen Ausführung von Vorgängen beruhen [...]."

Aus all dem folgt, dass ein KI-System eben ein „Mehr" sein muss als Maschine Learning oder wissens- und logikgestützte Konzepte. Ein KI-System muss Schlussfolgerungen treffen können, die nicht auf von Menschen vorher festgelegten Regeln (Algorithmen oder Konzepten) beruhen, es muss diese selbst lernen, also ableiten können.

Meiner Auffassung nach existiert damit derzeit (auf dem Markt) keine KI im Sinne der KI-Verordnung. Aber das kann sich zum einen sehr schnell ändern. Zum anderen kann man über die These, es gäbe noch keine KI im Sinne der KI-Verordnung naturgemäß trefflich streiten und – schon aufgrund der offensichtlich vorhanden Graubereiche – wohl andere Auslegungen vertreten.

Dabei erlaube ich mir aber an dieser Stelle den Hinweis, dass auch ChatGPT als sogenanntes „General Purpose Artificial Intelligence System", kurz GPAI, derzeit vermutlich noch nicht unter die KI-Verordnung fällt. Hier wird nämlich eine regulierungsbedürftige KI vermutet, wenn die gemessenen Floating Point Operations (FLOPs) größer als 10^25 sind. Es wird derzeit geschätzt, dass ChatGPT 4 bei 10^23 bis maximal 10^25 FLOPs liegt und demnach eben auch nicht unter die KI-Verordnung fiele.

Anders ausgedrückt: Die Definition von KI in der KI-Verordnung ist zukunftsgerichtet und soll verhindern, dass jede Software-Anwendung künftig sogleich als (regelungsbedürftiges) KI-System betrachtet wird.

2. Warum muss sich gerade HR mit der KI-Verordnung beschäftigen?

Neben der Frage, ob überhaupt ein KI-System im Sinne der Verordnung vorliegt, ist eine zweite Frage hochrelevant. Nämlich, die, ob ein „High Risk AI-System", also ob ein Hochrisiko-KI-System vorliegt. Denn nur über diese (sowie die GPAI-Systeme) breitet die KI-Verordnung ein strenges Reglementierungskorsett aus.

2.1. KI-Systeme im Personalbereich gelten als Hochrisiko-KI-Systeme

Die KI-Verordnung definiert nicht nur, was im Rahmen der Verordnung als KI gilt, sondern auch in Art. 6 Abs. 2 in Verbindung mit Annex III, wann beziehungsweise in welchen

[7] Die Autorin bezieht sich in diesem Artikel stets auf die im Trilog-Verfahren abgestimmte Fassung der KI-Verordnung, die am 24.01.2024 der Öffentlichkeit vorgestellt wurde: https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-FullText.pdf.

Bereichen ein KI-System als Hochrisiko-System zu betrachten ist. Hier heißt es in Annex III, Ziffer 4:

4) Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit

a) KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden sollen, insbesondere zur Schaltung gezielter Stellenanzeigen, zur Analyse und Filterung von Bewerbungen und zur Bewertung von Bewerbern;

b) KI-Systeme, die dazu verwendet werden sollen, Entscheidungen zu treffen, die sich auf die Bedingungen des Arbeitsverhältnisses, die Beförderung und die Beendigung von Arbeitsvertragsverhältnissen auswirken, Aufgaben auf der Grundlage von individuellem Verhalten oder persönlichen Eigenschaften oder Merkmalen zuzuweisen und die Leistung und das Verhalten von Personen in solchen Verhältnissen zu überwachen und zu bewerten sowie das Verhalten von Personen in entsprechenden Beschäftigungsverhältnissen zu beobachten und zu bewerten.

KI-Systeme im Personalbereich gelten also grundsätzlich als Hochrisiko-Systeme.

2.2. Pflichten beim Betreiben von Hochrisiko-KI-Systeme

Die Betreiber von Hochrisiko-KI-Systemen unterliegen mannigfaltigen Anforderungen. Diese können im Rahmen dieses Artikels nicht alle dargestellt werden. Aber allein die nachfolgend beschriebenen „Allgemeinen Pflichten" der Art. 9 bis 15 KI-VO geben einen guten Eindruck davon, wie regelungsintensiv der Einsatz von Hochrisiko-KI - zu Recht - sein wird:

Nach Art. 9 ist ein Risikomanagement zur steten Ermittlung von Risiken und dem schnellen Ergreifen von Maßnahmen als iterativer Prozess über den gesamten Lebenszyklus der KI zu betreiben.

Art. 10 verlangt eine strenge Data-Governance. Die Trainings-, Validierungs- und Testdatensätze müssen hohe Qualitätskriterien hinsichtlich der Herkunft, etwaiger Anreicherungen, der Relevanz und Zweckbezogenheit sowie der Vollständigkeit erfüllen. Dazu sind Merkmale berücksichtigen, die für das spezifische geografische, kontextuelle, verhaltensbezogene oder funktionale Umfeld des Zwecks des KI-Systems bedeutsam sind.

Vor dem Inverkehrbringen des Hochrisiko-Systems ist nach Art. 11 eine umfassende technische Dokumentation zu erstellen.

Während des gesamten Lebenszyklus ist nach Art. 12 eine fortlaufende Log-Protokollierung vorzunehmen, um die Funktionsweise der KI rückverfolgen und so gegebenenfalls Fehler erkennen und beseitigen zu können.

Art. 13 verlangt wiederum, Hochrisiko Systeme derart transparent zu entwickeln, das Nutzer des Systems die Ergebnisse interpretieren und – mittels beizuliegenden Gebrauchsanweisungen - ihrerseits den Endnutzern gegenüber ihren Informationspflichten nachkommen können.

Weiter muss ein solches System gemäß Art. 14 durch eine kompetente menschliche Aufsicht, die in der Lage sein muss, Anomalien zu erkennen sowie zu beheben, fortlaufend überwacht werden.

Und schließlich muss die IT-Sicherheit, hier Cybersicherheit genannt, fortlaufend gem. Art. 15 gewährleistet sein.

2.3. Folgen bei Verstößen gegen die KI-Verordnung

Verstöße gegen die vorgenannten Pflichten sind mit Bußgeldern von bis zu 15 Millionen Euro oder bis zu 3 Prozent des weltweiten Jahresumsatzes bewehrt. Daneben sind auch andere Maßnahmen wie die Untersagung der weiteren Verwendung von KI-Systemen möglich.

2.4. Ab wann gilt das alles?

Die KI-Verordnung soll im April 2024 vom EU-Parlament verabschiedet werden und tritt voraussichtlich im Frühsommer in Kraft. Regelungen in Bezug auf Hochrisiko-Systeme erlangen aber erst nach weiteren 36 Monaten Geltung.

2.5. Gibt es keine Ausnahmen?

Schon in der Universität wird den Student*innen eingebläut, Paragrafen bis zum Ende zu lesen. Schließlich kann

sich in einem der hinteren Absätze immer noch eine Ausnahme verbergen, so auch hier. Im derzeitigen Art. 6 Abs. 2a KI-VO heißt es:

(2a) Abweichend von Absatz 2 gelten KI-Systeme nicht als mit hohem Risiko behaftet, [...] wenn eines oder mehrere der folgenden Kriterien erfüllt sind:

a) Das KI-System ist dazu bestimmt, eine enge verfahrenstechnische Aufgabe zu erfüllen;

b) das KI-System ist dazu bestimmt, das Ergebnis einer zuvor ausgeführten menschlichen Tätigkeit zu verbessern;

c) das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, und ist nicht dazu bestimmt, die zuvor durchgeführte menschliche Bewertung, ohne angemessene menschliche Überprüfung zu ersetzen oder zu beeinflussen; oder

d) das KI-System soll eine vorbereitende Aufgabe für eine Bewertung übernehmen, die für den Zweck der in Anhang III aufgeführten Anwendungsfälle relevant ist.

Gerade im Bereich der Personalarbeit sind Anwendungen denkbar, die unter diese Ausnahmen fallen können: Ein Lebenslauf-Parsing nach Noten wäre etwa eine enge verfahrenstechnische Aufgabe. Der Einsatz eines Online-Assessments könnte unter Ziffer b) fallen, da es hilft, den Auswahlprozess zu verbessern, in dem Bauchgefühle durch wissenschaftlich validierte Eignungsdiagnostik ersetzt werden. KI im Personalcontrolling könnte gegebenenfalls genderbasierte Abweichungen in Gehaltserhöhungen erkennen (Ziffer c)) oder aber Beschäftigte für Personalentwicklungsmaßnahmen identifizieren (Ziffer d)).

Selbst wenn eine KI-Anwendung also die Personalarbeit unterstützen sollte, bedeutet das nicht zwingend, dass eine solche als Hochrisiko-KI-Anwendung einzustufen ist. Gemäß Art. 6 Abs. 2b KI-VO muss eine solche Einschätzung allerdings dokumentiert und auf Anforderungen den Behörden übergeben werden.

3. Was bedeutet das alles konkret für das Personalwesen?

Entscheidend ist bei all dem natürlich nicht, ob eine Anwendung mit „KI“ in den Marketingunterlagen wirbt, sondern ob es sich um KI im Sinne der KI-Verordnung handelt. Es ist daher auch davon auszugehen, dass der derzeitige Hype, jeden hilfreichen Algorithmus als "KI" zu bewerben, mit Geltung der KI-Verordnung nachlassen wird.

Doch wie dem auch sei, wenn im Personalwesen „KI“-Anwendungen eingesetzt werden sollen, muss vor der Geltung der KI-Verordnung beziehungsweise, sollte die KI-Verordnung bereits Geltung erlangt haben, vor der Anschaffung und dem Einsatz der jeweiligen Anwendung zwingend geprüft werden, ob es sich dabei um

- ein KI-System im Sinne der KI-Verordnung handelt.

Wenn dies eindeutig nicht der Fall ist, muss die Software-Anwendung nur die üblichen datenschutz- und arbeitsrechtlichen Anforderungen erfüllen. Wenn die Frage, ob es sich um ein KI-System im Sinne der KI-Verordnung handelt, nicht hinreichend verneint werden kann, dann muss weiter geprüft werden,

- ob es sich um ein Hochrisiko-KI-System handelt, das ausnahmsweise nach Art. 6 Abs. 2a KI-VO nicht als mit hohem Risiko behaftet gilt.

Wenn auch dies verneint werden muss und es sich somit um eine Hochrisiko-KI im Bereich der Personalarbeit handelt, sind alle (oben genannten) Anforderungen und Pflichten der KI-Verordnung zu erfüllen.

Anders ausgedrückt: Personalleiter*innen obliegen bei der Nutzung oder Einführung von Software-Anwendungen, die KI-Systeme beinhalten könnten, neuen Verantwortlichkeiten nach der KI-Verordnung zum Schutz ihrer Beschäftigten einschließlich der Bewerber*innen. Kommen sie diesen nicht nach, kann das erhebliche Folgen für die Arbeit in der Personalabteilung sowie aufgrund der im Raum stehenden Bußgelder für das gesamte Unternehmen haben.

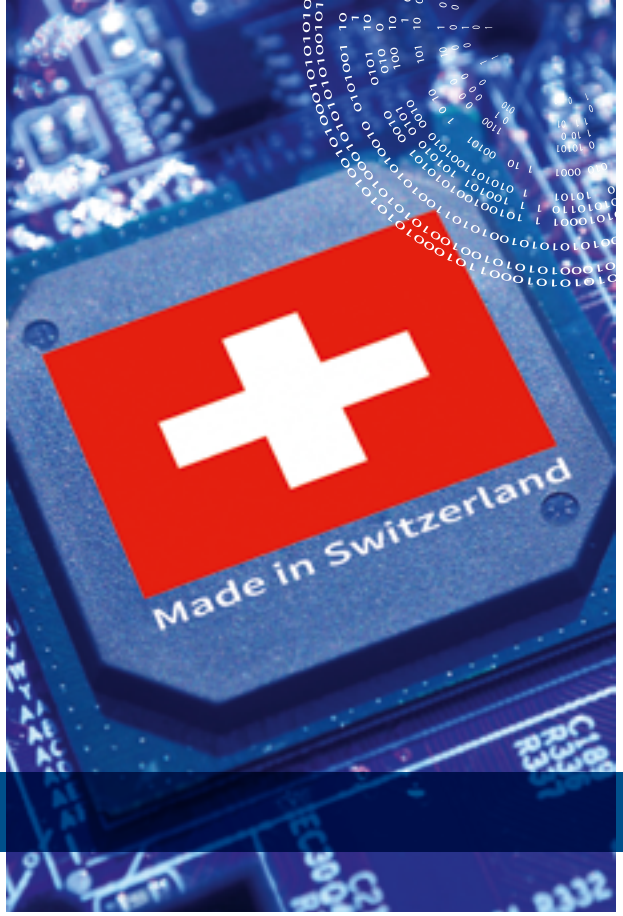
In diesem Sinne: Digitale Personalarbeit mit Hilfe von KI bleibt tatsächlich wie rechtlich spannend!

Über die Autorin

Nina Diercks, M.Litt (University of Aberdeen)
ist seit 2010 als Rechtsanwältin tätig und führt die Anwaltskanzlei Diercks in Hamburg. Sie arbeitet bundesweit, jedoch ausschließlich in den Bereichen des IT- | Datenschutz- und des angrenzenden Arbeitsrechts. Daneben veröffentlicht Nina Diercks regelmäßig Fachbeiträge und betreibt – ebenfalls seit 2010 – den Blog Diercks Digital Recht. Dazu ist sie als (Fach-)Referentin, Interviewpartnerin und (Gast-)Autorin gefragt.

▶ www.anwaltskanzlei-diercks.de

ANWALTSKANZLEI DIERCKS



DAS REVIDIERTE DATENSCHUTZ-RECHT DER SCHWEIZ

Dr. David Vasella

1. Weshalb das DSG revidiert wurde

Das schweizerische materielle Datenschutzrecht ist zersplittert: Für private Unternehmen und für Bundesorgane gilt in erster Linie das Bundesgesetz über den Datenschutz («DSG»), für Behörden auf kantonaler Ebene und in den Gemeinden gelten jeweils kantonale Datenschutzgesetze. Dazu kommt eine Vielzahl sektorieller Regelungen. Das in der Praxis aber wohl bedeutendste Gesetz bleibt das DSG. Es wird durch Verordnungen ergänzt und konkretisiert, vor allem durch die Datenschutzverordnung («DSV»).

Das alte DSG war Ende der 80er Jahre geschaffen worden und 1992 in Kraft getreten. Seither hat sich Welt verändert, die Digitalisierung und damit die Risiken schwer absehbarer Datenauswertungen sind explodiert. Die Instrumente des alten DSG waren dem nicht gewachsen: Weder sah es ausreichende Vollzugsinstrumente vor, noch kannte es eine eigentliche Governance. Die Einhaltung des DSG beruhte deshalb vor allem auf dem guten Willen der Unternehmen und ihren sehr unterschiedlich ausgeprägten Reputationsrisiken; der Ausdruck «Vollzugsdefizit» war sicher nicht falsch. Auch waren internationale Entwicklungen nachzuvollziehen. Das betrifft die Schengen-Bestimmungen und die Revision der Europaratskonvention 108 (ERK 108), die für die Schweiz verbindlich sind, aber natürlich auch die DSGVO. Die Sorge um die Angemessenheit des schweizerischen Rechts, die die EU-Kommission erst kürzlich bestätigt hat, und die Bedeutung der DSGVO als extraterritorial anwendbare Rechtsordnung, als Schrittmacher der internationalen Entwicklung und als Referenzrahmen der datenschutzrechtlichen Diskussion haben eine gewisse Angleichung unausweichlich gemacht.

Nach jahrelangen Vorarbeiten sind das totalrevidierte DSG und die ebenfalls totalrevidierte DSV am 1. September 2023 in Kraft getreten. Sie gelten seither, weitgehend ohne Übergangsfristen.

2. Was die Revision gebracht hat

Die Revision verfolgte im Wesentlichen drei Ziele: Sie sollte die Anwendung und Durchsetzung des DSG verbessern, die Transparenz der Datenbearbeitungen fördern (das DSG spricht von «bearbeiten» und von «Personendaten» statt von «verarbeiten» und «personenbezogenen Daten») und den Abstand zur DSGVO und zur ERK 108 verringern. Das ist zumindest teilweise gelungen, auch wenn das revidierte Recht, ähnlich wie die DSGVO, zu Rechtsunsicherheit führt.

Die schweizerische Aufsichtsbehörde auf Bundesebene ist der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte («EDÖB»; «Öffentlichkeitsbeauftragter» bezieht sich auf seine Aufgaben im schweizerischen Informationsfreiheitsrecht). Das neue DSG stattet ihn mit größeren Kompetenzen aus: Im privaten Bereich konnte er bisher nur Untersuchungen durchführen, wenn Verletzungen mit einer gewissen Breitenwirkung zur Diskussion standen, und er konnte Untersuchungen nur mit unverbindlichen Empfehlungen abschließen. Erst die Gerichte konnten verbindliche Anweisungen erlassen. Mit dem neuen Recht ist der EDÖB bei Untersuchungen etwas freier, und vor allem kann er nun – unter anderem – die Anpassung oder Einstellung von Datenbearbeitungen verfügen.

Neu sind ebenfalls Bestimmungen zur Informationspflicht. Das alte Recht kannte eine solche – über den Transparenz-

grundsatz hinaus – nur bei bestimmten besonders riskanten Bearbeitungen. Nun gilt eine Informationspflicht, die mit jener von Art. 13 Abs. 1 f. DSGVO vergleichbar ist. Die Anforderungen sind allerdings etwas niedriger, die Ausnahmen etwas grosszügiger. Datenschutzerklärungen, die der DSGVO entsprechen, müssen für die Schweiz daher nur punktuell angepasst werden – in Details aber durchaus. Auch bei den weiteren Betroffenenrechten wirkt die Revision verschärfend: Das Auskunftsrecht kannte auch das alte DSG, es wurde aber etwas breiter angewendet, und neu ist das Recht auf Datenportabilität.

Für private Unternehmen ebenfalls neu sind Pflichten, die man der Governance und der Datensicherheit zuordnen kann: Sie müssen Bearbeitungsverzeichnisse führen (es gibt hier kaum Unterschiede zu Art. 12 DSGVO) und bei voraussichtlich hohen Risiken für Betroffene eine Datenschutzfolgenabschätzung durchführen (auch hier sind die Unterschiede zur Regelung in der DSGVO klein), und Datensicherheitsverletzungen müssen unter Umständen dem EDÖB oder den betroffenen Personen mitgeteilt werden.

3. Wie sich das DSG weiterhin von der DSGVO unterscheidet

Da die DSGVO für die Schweiz nicht verbindlich ist, kann die entsprechende Praxis nicht unbesehen übernommen werden. Das DSG verfolgt auch einen auffallend anderen Regelungsansatz als die DSGVO. Es beruht nicht auf dem Verbotsprinzip, sondern erlaubt eine Bearbeitung von Personendaten grundsätzlich, solange die allgemeinen Grundsätze der Bearbeitung (die weitgehend Art. 5 Abs. 1 DSGVO entsprechen) eingehalten werden. In der Praxis bedeutet dies nicht nur mehr Realismus, sondern vor allem, dass häufiger auf Einwilligungen verzichtet werden darf.

Allgemein ist die DSGVO formalistischer als das DSG. Letzteres kennt etwa keinen allgemeinen «Accountability»-Grundsatz – es kommt also weder zu einer Beweislastumkehr noch stellt fehlende Nachweisbarkeit einen eigenständigen Verstoss gegen das DSG dar.

Auch anderswo bestehen Unterschiede, etwa beim Kopplungsverbot, das in der Schweiz bewusst nicht übernommen wurde, bei den Betroffenenrechten, die kein eigentliches Erleichterungsgebot kennen, bei der Meldepflicht von Sicherheitsverletzungen, deren Schwelle höher angesetzt ist, oder beim Datenschutzberater – dem Äquivalent zum Datenschutzbeauftragten –, dessen Bestellung im Privatbereich in allen Fällen freiwillig ist.

Ein weiterer Unterschied besteht in der Behördenpraxis. Aufsichtsbehörden in der EU agieren zwar mit unterschiedlichem Impetus, sind aber erheblich aktiver und meist auch strenger als der EDÖB. Letzterer sieht sich in der Praxis erfahrungsgemäss weniger als Regulator und mehr als pragmatische Aufsichts- und Beratungsbehörde. Entsprechend fallen seine Stellungnahmen meist lebensnäher aus; dafür sind sie teilweise nur lose ans DSG angelehnt. In letzter Zeit lässt sich allerdings eine gewisse Verschärfung seiner Praxis beobachten.

Strenger als die DSGVO ist das DSG nur in wenigen Punkten, etwa bei der Informationspflicht (bei einer Übermittlung ins Ausland sind die Empfängerstaaten zu nennen, selbst bei Angemessenheit) oder bei der Protokollierung hochriskanter Datenbearbeitungen.

4. Wann das DSG anwendbar ist

Es ist nicht ganz einfach den räumlichen Anwendungsbereich des DSG zu bestimmen, weil abhängig von der Rechtsnatur unterschiedliche kollisionsrechtliche Regeln gelten. Für Bestimmungen privatrechtlicher Natur wie beispielsweise jene über die Bearbeitungsgrundsätze oder Betroffenenrechte besitzt die betroffene Person ein Wahlrecht, sofern ein Gericht in der Schweiz zuständig ist. Sie kann – vereinfacht ausgedrückt – wählen, ob sie ihr Heimatrecht zur Anwendung bringen oder sich auf das Recht des Verantwortlichen oder Auftragsbearbeiters berufen will, dem sie eine Datenschutzverletzung vorwirft. Unternehmen außerhalb der Schweiz müssen deshalb damit rechnen, dem DSG unterstellt zu sein, soweit sie Personendaten von Personen in der Schweiz nicht nur zufällig oder ganz vereinzelt bearbeiten.

Andere Regelungen sind öffentlich-rechtlicher Natur, so die Bestimmungen über den EDÖB, aber auch die Informationspflicht oder die Governance-Pflichten. Das DSG gilt hier, wenn eine Datenbearbeitung von einer Niederlassung in der Schweiz veranlasst wurde (etwa von einer Tochter oder Zweigniederlassung) oder wenn eine Bearbeitung eine ausreichende Auswirkung auf die Schweiz hat. Im Sinne einer Faustregel trifft letzteres zu, wenn der Verantwortliche oder Auftragsbearbeiter seine Tätigkeit auf die Schweiz ausrichtet.

Im Ergebnis ist also maßgeben, ob eine Datenbearbeitung mit einer gewissen Ausrichtung auf die Schweiz verbunden ist. Ist das DSG in diesem Sinne anwendbar, können es auch die strafrechtlichen Bestimmungen sein.

Das DSG kennt eine Pflicht ausländischer Unternehmen einen Vertreter in der Schweiz zu bestimmen. Man hat sich hier an Art. 3 und 27 DSGVO angelehnt. Sie gilt allerdings nur, wenn eine Bearbeitung von Personendaten Personen in der Schweiz betrifft, im Zusammenhang mit dem Angebot von Waren und Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz steht, umfangreich und regelmässig ist und zu einem hohen Risiko für die Be-

troffenen führt. Diese Bedingungen sind reichlich vage, und bisher ist kaum geklärt, wie weit die Vertreterpflicht reicht. Es wurden jedenfalls erst wenige Vertretungen bestellt.

5. Welche Rechtsrisiken bestehen

Die Risiken im Fall einer Verletzung des Datenschutzrechts sind nicht nur rechtlichen Ursprungs – im Vordergrund stehen weiterhin Reputationsrisiken und die Sorge um das Kundenvertrauen. Die Rechtsrisiken haben sich mit der Revision des DSG aber deutlich erhöht.

Wie bereits erwähnt hat der EDÖB nun die Möglichkeit Datenbearbeitungen zu untersagen oder eine Anpassung zu verfügen. Bisher ist er nicht allzu aktiv. Es wurden zwar Untersuchungen nach neuem Recht eingeleitet, aber – soweit bekannt – noch nicht durch Verfügungen abgeschlossen. Aber natürlich steht der EDÖB unter einem gewissen Druck von den erweiterten Kompetenzen auch Gebrauch zu machen, und in letzter Zeit ist eine gewisse Verschärfung zu beobachten.

Dazu kommen strafrechtliche Sanktionen. Der Gesetzgeber hat bewusst davon Abstand genommen Unternehmensbußen vorzusehen. Stattdessen können bestimmte Verletzungen mit Buße bis zu CHF 250'000 bestraft werden (faktisch sind diese Bußen nicht versicherbar), und zudem droht ein Eintrag im Strafregister. Dabei sind es nicht etwa die Unternehmen, die gebüßt würden, sondern diejenigen Personen, die innerhalb des Unternehmens für den Verstoß verantwortlich sind.

Nur ausnahmsweise kann eine Buße dem Unternehmen auferlegt werden: Wenn sie den Betrag von 50.000 CHF nicht übersteigt und der Aufwand zur Ermittlung der verantwortlichen Person unverhältnismässig wäre. Die Risiken treffen daher in erster Linie Business-Funktionen (etwa Marketingleiter oder Personen im Bereich HR, die beispielsweise die Korrektheit einer Datenschutzerklärung prüfen), aber auch jede andere Person, solange die entsprechende Entscheidung von ihr getroffen wurde. Auch ein Datenschutzberater ist nicht vor Bußen gefeit, sofern er für einen Verstoß verantwortlich ist – ist er tatsächlich unabhängig, sollte dies aber eine Ausnahme sein.

Jedenfalls setzt eine Buße voraus, dass die entsprechende Verletzung strafbedroht ist. Das trifft zum Beispiel auf falsche Angaben in Datenschutzerklärungen oder in einer Auskunft zu, ebenso wie für eine unzulässige Übermittlung ins Ausland oder eine Auftragsbearbeitung ohne entsprechende Vereinbarung, nicht aber auf eine unterlassene DSFA, eine unterlassene Meldung einer Sicherheitsverletzung oder eine zu Unrecht verweigerte Auskunft. Unklar ist die Lage im Bereich der Datensicherheit: Zwar ist eine Verletzung der Mindestanforderungen an die Datensicherheit grundsätzlich strafbar, aber es ist offen, ob es dem Gesetzgeber tatsächlich gelungen ist solche Mindestanforderungen zu formulieren; die Anforderungen an die Sicherheit sind weitgehend programmatischer Natur.

Strafbar sind nur vorsätzliche Verstöße. Das schließt zwar den Eventualvorsatz ein, die bewusste Inkaufnahme der Verletzung, aber nicht schon Nachlässigkeiten. Und schließlich setzt die Verfolgung einer Verletzung in fast allen Fällen einen Strafantrag voraus. Die Strafverfolgung liegt dabei bei den Kantonen, nicht beim EDÖB, und bisher sind keine Strafverfahren wegen Verletzungen des DSG bekannt. Es bleibt dennoch ein Unbehagen, besonders wegen der sehr offen formulierten Tatbestände.

Nicht ausgeschlossen ist ferner eine zivilrechtliche Haftung gegenüber den Betroffenen. Das DSG kennt allerdings keinen immateriellen Schadenersatz, und der erforderliche, konkrete Nachweis eines Schadens ist oft nicht möglich. Schadenersatzrisiken sind deshalb meist niedrig. Aber selbstverständlich kann eine Datenschutzverletzung zugleich eine Vertragsverletzung bedeuten, mit den entsprechenden Folgen.

6. Was Unternehmen im Ausland tun sollten

Unternehmen im Ausland sollten prüfen, wenn ihre Bearbeitungen einen Bezug zur Schweiz haben, ob diese in Zusammenhang mit einer gewissen Ausrichtung auf die Schweiz steht. Trifft dies zu und ist das DSG entsprechend anwendbar, kann das Unternehmen zunächst von den bestehenden Compliance-Maßnahmen ausgehen. Es wird kaum Dokumentation oder Prozesse benötigen, die nicht auch unter der DSGVO erforderlich wären.

Allerdings werden Anpassungen erforderlich sein. Das betrifft zunächst den Anwendungsbereich interner Vorgaben, Prozesse und Verzeichnisse international tätiger Unternehmen oder Gruppen, die nicht auf die DSGVO beziehungsweise das EWR-Gebiet beschränkt sind. Auch ihr Inhalt sollte die Schweiz einschliessen – so sollten Prozessbeschreibungen für den Umgang mit Sicherheitsverletzungen auch die Meldung an den EDÖB und an Betroffene in der Schweiz abdecken, und Bearbeitungsverzeichnisse sollten auch lokale Bearbeitungen abdecken. Es spricht aber nichts dagegen die Bearbeitungen schweizerischer Gesellschaften in einem übergreifenden Verzeichnis zu erfassen.

Auch inhaltlich werden sich gewisse Anpassungen aufdrängen. Datenschutzerklärungen etwa sind zu prüfen, weil das DSG hier in wenigen Punkten etwas strenger ist. Auch bei Prozessbeschreibungen sind Abweichungen des DSG zu berücksichtigen. Beispielsweise ist die Regelung des Auskunftsrechts etwas anders, und vor allem sind die Verwei-

gerungsgründe weiter gefasst. Schliesslich sollte das DSG bei Richtlinien und Verträgen wie etwa bei ADV, der Vereinbarung gemeinsam Verantwortlicher oder den üblichen gruppenweiten Rahmenvereinbarungen abgedeckt werden – dies nicht nur, um formal die Schweiz zu berücksichtigen, sondern unter Umständen auch, um die etwas weiteren Spielräume des DSG zu nutzen (sofern ein international tätiges Unternehmen nicht weltweit denselben Standard aufrechterhalten will, was allerdings häufig zu beobachten ist). Die Anforderungen an Richtlinien und Verträge unterscheiden sich aber kaum; auch die Standardvertragsklauseln können für Exporte aus der Schweiz verwendet werden, mit kleineren Anpassungen.

In organisatorischer Hinsicht wird der Anpassungsaufwand niedrig sein, unter anderem weil das DSG nicht verlangt, einen Datenschutzberater zu bestellen. Entscheidet sich ein Unternehmen freiwillig für einen Datenschutzberater, kann dessen Funktion grundsätzlich auch von einem ausländischen Datenschutzverantwortlichen erfüllt werden, sofern dieser ausreichend mit dem DSG vertraut ist und bei Bedarf in die Schweiz reisen kann. Bei Schulungen schliesslich werden Mitarbeitende in der Schweiz oft besonders geschult (auch wenn das DSG dies nicht verlangt), häufig auch in Ergänzung zu einer bestehenden allgemeinen Schulung.

7. Was noch kommt

Die Revision des DSG ist abgeschlossen, aber nicht die Evolution des Datenschutzrechts. Es ist absehbar, dass sich die Praxis weiter dem europäischen Recht annähert, besonders der DSGVO, auch wenn sie für die Schweiz rechtlich betrachtet nicht maßgebend ist. Die Entscheidungen des EuGH werden stark beachtet, ebenso wie Leitlinien des EDSA oder Handlungsanweisungen ausländischer (besonders deutscher) Aufsichtsbehörden. Kaum eine datenschutzrechtliche Prüfung kommt ohne einen Blick auf die DSGVO aus – aus diesem Grund begleiten wir die Entwicklung des Europäischen Datenschutzrechts auf www.datenrecht.ch. Es ist absehbar, dass sich die Praxis des DSG jener der DSGVO bis zu einem gewissen Grad annähern wird, auch wenn man das bedauern muss.

Die weiteren Regulierungen der EU ziehen an der Schweiz nicht spurlos vorüber, sei es, weil sie einen extraterritorialen Anwendungsbereich haben wie etwa der Digital Services Act, die KI-Verordnung, DORA und andere Erlasse, sei es, weil die Schweiz mit parallelen Regelungen nachzieht. Sie plant beispielsweise die Regulierung großer Kommunikationsplattformen; bis Ende März 2024 will der Bundesrat einen Vorschlag unterbreiten. Bei der Regulierung der künstlichen Intelligenz ist die Schweiz kein Vorreiter, aber bis Ende 2024 soll auch hier mehr Klarheit über das weitere Vorgehen herrschen. Es wäre keine Überraschung, wenn sich die Schweiz an die KI-Verordnung anlehnt.

Über den Autor

Dr. David Vasella
ist Rechtsanwalt, CIPP/E, CIPM, FIP,
Partner bei Walder Wyss AG, Zürich

Anzeige

Piltz Legal update
Seminare und Veranstaltungen von Piltz Legal

Fränkischer Datenschutztag – Würzburg, Schlosshotel Steinburg
12.06.2024: Welcome Event ab 18:00 Uhr / 13.06.2024 Hauptveranstaltung ab 9:00 Uhr

Aktuelle datenschutzrechtliche Entwicklungen, Ansichten und Empfehlungen der Aufsichtsbehörden sowie hilfreiche Praxiserfahrungen.

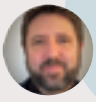
Eröffnungsrede
Michael Will – Präsident Bayerisches Landesamt für Datenschutzaufsicht

Von der analogen zur digitalen Kontrolle am Arbeitsplatz - Neues zu Beschäftigtendatenschutz und Künstlicher Intelligenz
Dr. Stefan Brink – Geschäftsführender Direktor, Institut wida/ Berlin

Datenschutz im Mittelstand, oder: Der DSB als glücklicher Sisyphus
Dr. Philip Laue – Datenschutzbeauftragter der ZWILLING J.A. Henckels AG

Aktuelle Anforderungen an den „Stand der Technik" im Rahmen des Art. 32 DSGVO
Prof. Ronald Petrlic – Professor für Informationssicherheit an der TH Nürnberg

Aktuelles zu DSGVO-Betroffenenrechten
Dr. Carlo Piltz – Rechtsanwalt, Partner bei Piltz Legal



Aktuelle Risiken im Bereich der Cybersicherheit und mögliche Schutzmaßnahmen aus Datenschutzperspektive
Andreas Sachs – Vizepräsident Bayerisches Landesamt für Datenschutzaufsicht

Money, Money, Money: FAQ zu TTDSG und Bußgeldern
Dr. Nina Herbort – Berliner Beauftragte für Datenschutz und Informationsfreiheit
&
Henrike Teitge – Referentin im Bereich Sanktionen bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Teilnahmegebühr

Early Bird bis zum 31.03.2024	349,00 EUR (netto)
Ab dem 01.04.2024	429,00 EUR (netto)

Weitere Informationen

Piltz Rechtsanwälte PartGmbB | +49 30 814 53 50 00 | events@piltz.legal | www.piltz.legal

ALEXANDER ROSSNAGEL, MARIA CHRISTINA ROST

DER EUGH ZU SCORING UND AUTOMATISIERTEN ENTSCHEIDUNGEN

Die Mitglieder des Gerichtshofs im Juni 2022. (Foto: Gerichtshof der Europäischen Union)

Mit zwei Urteilen entschied der EuGH am 7.12.2023 über die Zulässigkeit der Erhebung und Speicherung von personenbezogenen Daten aus öffentlichen Registern und über die automatisierte Erstellung von Scorewerten und damit über wichtige Fragen zur Arbeitsweise von Auskunfteien. Daneben entschied der EuGH auch über den Charakter von Beschwerden und Verhaltensregeln. Beide Entscheidungen haben weit über Auskunfteien hinaus Auswirkungen.

I. EuGH-Urteil zur Speicherung von Daten aus öffentlichen Registern

In der Entscheidung C-26/22 und C-64/22[1] hatte sich der EuGH mit fünf Vorlagefragen des Verwaltungsgerichts Wiesbaden zu befassen. Im Ausgangsverfahren ging es darum, ob Auskunfteien Daten zu einer Restschuldbefreiung für drei Jahre speichern dürfen, die sie aus dem Insolvenzregister übernommen haben.

1. Berechtigte Interesse

Maßstab für den EuGH war Art. 6 UAbs. 1 Buchst. f DSGVO. Diesen Erlaubnistatbestand prüfte der EuGH in drei Stufen. In der ersten Stufe bejaht er die berechtigten Interessen der Auskunftei und der Kreditwirtschaft. Hierfür nahm er Bezug auf EU-Regelungen zu Verbraucherschutz und Immobilienkrediten und auf das „reibungslose Funktionieren des gesamten Kreditsystems" (Rn. 83 – 86). Für die zweite Stufe verweist der EuGH darauf, dass die Datenverarbeitung auf das unbedingt Notwendige zur Verwirklichung des berechtigten Interesses zu beschränken ist (Rn. 87). Die Prüfung der Erforderlichkeit verbindet er mit der dritten Stufe, der Abwägung der gegensätzlichen Interessen.

2. Interessenabwägung

Zugunsten der Auskunfteien ist im Rahmen der Abwägung der Interessen zu berücksichtigen, dass die objektive und

[1] EuGH von 7.12.2023, C 26/22 und C-64/22 – ECLI:EU:C:2023:958 – Schufa I, https://curia.europa.eu/juris/liste.jsf?language=de&td=ALL&num=C-26/22

zuverlässige Bewertung der Kreditwürdigkeit es der Auskunftei ermöglicht „Informationsunterschiede auszugleichen und damit Betrugsrisiken und andere Unsicherheiten zu verringern“ (Rn. 93). Aber auch das Insolvenzregister zielt auf „eine bessere Information der betroffenen Gläubiger und Gerichte“ ab (Rn. 96), was das Interesse an einer zusätzlichen Speicherung reduziert.

Für die Bewertung der Auswirkungen der Speicherung der Daten in der Auskunftei sind dem EuGH zwei Aspekte wichtig. Erstens führt es zu einer Vervielfältigung des Grundrechtseingriffs, dass die Daten nicht nur im öffentlichen Register, sondern auch in den Datenbanken mehrerer Auskunfteien gespeichert werden. Zweitens erfolgt diese Speicherung nicht aus konkretem Anlass, sondern auf Vorrat für den Fall, dass Vertragspartner der Auskunfteien Auskünfte anfragen (Rn. 89). Vor allem aber ist zu berücksichtigen, dass die „Verarbeitung von Daten über eine Restschuldbefreiung, wie etwa die Speicherung, Analyse und Weitergabe dieser Daten an einen Dritten“, „einen schweren Eingriff in die Grundrechte der betroffenen Person“ darstellt (Rn. 94). Solche Daten dienen als negativer Faktor bei der Beurteilung der Kreditwürdigkeit der betroffenen Person und stellen daher sensible Informationen über ihr Privatleben dar. Die „Verarbeitung kann den Interessen der betroffenen Person beträchtlich schaden und die Ausübung ihrer Freiheiten erheblich erschweren, insbesondere wenn es darum geht, Grundbedürfnisse zu decken“. Die negativen Folgen für die betroffene Person sind „umso größer und die Anforderungen an die Rechtmäßigkeit der Speicherung dieser Informationen umso höher, je länger die Daten durch Wirtschaftsauskunfteien gespeichert werden“ (Rn. 95).

3. Gewichtung der Interessen

Bei der Gewichtung der entgegengesetzten Interessen nimmt der EuGH Bezug auf die Regelung in § 3 InsBekV[2], die für das öffentliche Register eine Speicherdauer von nur sechs Monaten vorsieht. Der deutsche Gesetzgeber geht „davon aus, dass nach Ablauf einer Frist von sechs Monaten die Rechte und Interessen der betroffenen Person diejenigen der Öffentlichkeit, über diese Information zu verfügen, überwiegen“ (Rn. 97). Für den EuGH ist entscheidend, dass die Restschuldbefreiung es dem Begünstigten ermöglicht, sich erneut am Wirtschaftsleben zu beteiligen. Die Verwirklichung dieses Ziels wäre jedoch gefährdet, wenn Auskunfteien zur Beurteilung der wirtschaftlichen Situation einer Person Daten über eine Restschuldbefreiung für einen Bonitätsscore verwenden könnten, nachdem sie aus dem öffentlichen Insolvenzregister gelöscht worden sind (Rn. 98). Der EuGH stellt daher fest, dass die Interessen des Kreditsektors, über Informationen hinsichtlich einer Restschuldbefreiung zu verfügen, keine Verarbeitung dieser Daten nach Ablauf der Frist für ihre Speicherung im öffentlichen Insolvenzregister rechtfertigen können. Eine Speicherung dieser Daten durch eine Auskunftei kann nach der Löschung dieser Daten aus einem öffentlichen Insolvenzregister nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO gestützt werden (Rn. 99).

Für die parallele Speicherung der Daten zur Restschuldbefreiung während ihrer Veröffentlichung im Insolvenzregister trifft der EuGH keine so klare Feststellung. Einerseits sind „die Auswirkungen einer parallel erfolgenden Speicherung zwar als weniger schwerwiegend an(zu)sehen als nach Ablauf der sechs Monate“. Andererseits stellt diese Speicherung einen Eingriff in die in den Art. 7 und 8 der Charta verankerten Rechte dar. Sie verstärkt den Eingriff in das Recht der Person auf Achtung des Privatlebens (Rn. 100). Daher hat das vorlegende Verwaltungsgericht Wiesbaden zu prüfen, ob die Vorratsspeicherung dieser Daten durch die Auskunftei auf das zur Verwirklichung des berechtigten Interesses unbedingt Erforderliche beschränkt ist, obwohl die fraglichen Daten im öffentlichen Register abgerufen werden können und ohne dass ein Wirtschaftsunternehmen in einem konkreten Fall um Auskunft ersucht hat (Rn. 91).

4. Bedeutung von Verhaltensregeln nach Art. 40 DS-GVO

Die Auskunftei hatte sich für die dreijährige Speicherung der Daten zur Restschuldbefreiung auf die genehmigten Verhaltensregeln des Verbands „Die Wirtschaftsauskunfteien“ gemäß Art. 40 DSGVO berufen. Zu solchen Verhaltensregeln stellt der EuGH nur fest, dass sie die Bedingungen der Rechtmäßigkeit der Datenverarbeitung nicht verändern, sondern nur für ihren Anwendungsbereich konkretisieren können. Daraus schließt er: „Verhaltensregeln, die zu einer anderen Beurteilung führen würden als derjenigen, die sich nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO ergibt, (können) bei der Abwägung nach dieser Bestimmung nicht berücksichtigt werden“ (Rn. 101 – 105).

5. Ermessen im Beschwerdeverfahren

Der EuGH hatte auch über den Charakter des Beschwerdeverfahrens zu entscheiden, der von deutschen Gerichten unterschiedlich beurteilt wurde. Nach Art. 78 Abs. 1 DSGVO unterliegt ein rechtsverbindlicher Beschluss einer Aufsichtsbehörde über eine Beschwerde einer vollständigen inhaltlichen Überprüfung durch das Gericht (Rn. 70). Diese betrifft die Feststellung des Sachverhalts und seine datenschutzrechtliche Bewertung. Dagegen geht der EuGH davon aus, dass die Datenschutzaufsichtsbehörde „hinsichtlich der in Art. 58 Abs. 2 DSGVO aufgezählten Abhilfebefugnisse über ein Ermessen in Bezug auf die geeigneten und erforderlichen Mittel verfügt“ (Rn. 68). Daher erfordert „die Gewährleistung eines wirksamen gerichtlichen Rechtsschutzes nicht,

[2] Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren und Restrukturierungssachen im Internet (InsBekV)

dass (das Gericht) befugt wäre, seine Beurteilung der Wahl der geeigneten und erforderlichen Abhilfebefugnisse an die Stelle der Beurteilung dieser Behörde zu setzen, sondern verlangt, dass dieses Gericht prüft, ob die Aufsichtsbehörde die Grenzen ihres Ermessens eingehalten hat" (Rn. 69).

II. EuGH-Urteil zur automatisierten Entscheidungsfindung durch Scoring

In der Entscheidung C-634/21[3] befasst sich der EuGH mit einer weiteren Vorlagefrage des Verwaltungsgerichts Wiesbaden. Dieses wollte wissen, ob die automatisierte Erstellung eines Wahrscheinlichkeitswerts über die Fähigkeit einer betroffenen Person, künftig einen Kredit zu bedienen, und die Übermittlung dieses Werts an ein Kreditinstitut, das über eine Kreditanfrage zu entscheiden hat, eine ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhende Entscheidung im Sinn des Art. 22 Abs. 1 DSGVO darstellt.

Für den EuGH hängt Art. 22 Abs. 1 DSGVO in seiner Anwendbarkeit von drei kumulativen Voraussetzungen ab. Es muss erstens eine „Entscheidung" vorliegen, zweitens muss diese Entscheidung „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – (beruhen)" und drittens muss sie „gegenüber (der betroffenen Person) rechtliche Wirkung entfalten" oder sie „in ähnlicher Weise erheblich" beeinträchtigen (Rn. 43).

Der Begriff „Entscheidung" ist nach dem EuGH weit auszulegen. Bereits aus dem Wortlaut des Art. 22 DSGVO ergibt sich, dass dieser Begriff sich nicht nur auf Handlungen bezieht, die rechtliche Wirkung gegenüber der betroffenen Person entfalten, sondern auch auf Handlungen, die diese Person in ähnlicher Weise erheblich beeinträchtigen (Rn. 44). Die weite Bedeutung des Begriffs „Entscheidung" wird von Erwägungsgrund 71 unterstützt. Danach umfasst der Begriff Entscheidung beispielsweise die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahrens ohne jegliches menschliche Eingreifen. Die Entscheidung kann aus einer Kette von mehreren Maßnahmen bestehen, nicht nur aus der diese Kette abschließenden Handlung. Entscheidend ist, ob auf die untersuchte Maßnahme die beiden anderen Voraussetzungen zutreffen.

Die zweite Voraussetzung ist, dass die Entscheidung ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht. Die Datensammlung der Auskunftei und die Erstellung des Wahrscheinlichkeitswerts erfüllen die Definition des „Profiling" in Art. 4 Nr. 4 DSGVO und damit auch die zweite Voraussetzung (Rn. 47).

Drittens muss die Entscheidung gegenüber der betroffenen Person „rechtliche Wirkung entfalten", oder sie „in ähnlicher Weise erheblich" beeinträchtigen. Entscheidend ist für den EuGH, ob das Handeln des Dritten, dem der Wahrscheinlichkeitswert übermittelt wird, „maßgeblich" von diesem Wert geleitet wird. Sofern der von einer Wirtschaftsauskunftei ermittelte und einer Bank mitgeteilte Wahrscheinlichkeitswert eine maßgebliche Rolle bei der Gewährung eines Kredits spielt ist die Ermittlung dieses Werts als solche als Entscheidung einzustufen, die im Sinne von Art. 22 Abs. 1 DSGVO gegenüber einer Person „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" (Rn. 50). Der EuGH stellt zusätzlich zu der Interpretation des Art. 22 Abs. 1 DSGVO zwei systematische Überlegungen an, um sein Ergebnis zu rechtfertigen.

Zum einen problematisiert er, dass Regelungen des Art. 22 DSGVO leerlaufen können, wenn nur die letzte Handlung in einer Entscheidungskette berücksichtigt würde, Entscheidungen in der Praxis aber in mehreren Schritten und arbeitsteilig getroffen werden. Er verweist dabei auf Abs. 2 (Voraussetzung für Aufhebung des Verbots), Abs. 3 (Garantien, wie das Recht auf Erwirkung des Eingreifens einer Person, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung) und Abs. 4 (keine besonderen Kategorien) (Rn. 53 – 55). Zum anderen verweist er auf Art. 13, 14 und 15 DS-GVO, nach denen „aussagekräftige Informationen über die involvierte Logik" zu geben sind, wenn eine Entscheidung nach Art. 22 Abs. 1 DSGVO vorliegt. Nur wenn „Entscheidung" so weit verstanden wird, wie der EuGH dies tut, greifen diese Regelungen. Ansonsten würde die Auskunftei keine Entscheidung treffen und das Kreditinstitut keine automatisierte Verarbeitung durchführen. Keiner von beiden müsste über die „involvierte Logik" informieren. Daher bestünde „die Gefahr einer Umgehung von Art. 22 DSGVO und folglich eine Rechtsschutzlücke" (Rn. 61). „In diesem Fall würde nämlich die Ermittlung eines Wahrscheinlichkeitswerts nicht den besonderen Anforderungen von Art. 22 Abs. 2 bis 4 DSGVO unterliegen, obwohl dieses Verfahren auf einer automatisierten Verarbeitung beruht und Wirkungen entfaltet, welche die betroffene Person erheblich beeinträchtigen, da das Handeln des Dritten (Bank), dem dieser Wahrscheinlichkeitswert übermittelt wird, von diesem maßgeblich geleitet ist." (Rn. 62).

Eine automatisierte Entscheidung ist nach Art. 22 Abs. 1 DSGVO grundsätzlich unzulässig und darf nur aufgrund einer Einwilligung oder einer gesetzlichen Erlaubnis getroffen werden. Nach Art. 22 Abs. 2 Buchst. b DSGVO kann das Scoring durch nationale Vorschriften gerechtfertigt sein. Der EuGH setzt sich mit den Anforderungen an die nationalen Vorschriften intensiv auseinander und betont insbesondere die Einhaltung von Art. 5 und 6 DS-GVO (Rn. 65 – 70). Bezüglich der Vereinbarkeit des § 31 BDSG mit dem Unionsrecht bestehen durchgreifende Bedenken.

[3] EuGH Urteil vom 7.12.2023, C-634/21 – ECLI:EU:C:2023:957 – Schufa II, https://curia.europa.eu/juris/liste.jsf?language=de&td=ALL&num=C-26/22

Sollte diese Bestimmung als mit dem Unionsrecht unvereinbar angesehen werden, würden die Auskunfteien nicht nur ohne Rechtsgrundlage handeln, sondern verstießen ipso iure gegen das in Art. 22 Abs. 1 DSGVO aufgestellte Verbot (Rn. 71). Es ist nun „Sache des vorlegenden Gerichts, zu prüfen, ob § 31 BDSG als Rechtsgrundlage im Sinne von Art. 22 Abs. 2 Buchst. b DSGVO qualifiziert werden kann. Sollte das vorlegende Gericht zu dem Schluss kommen, dass § 31 eine solche Rechtsgrundlage darstellt, hätte es noch zu prüfen, ob die in Art. 22 Abs. 2 Buchst. b und Abs. 4 DSGVO und in den Art. 5 und 6 DSGVO aufgestellten Anforderungen im vorliegenden Fall erfüllt sind."

Die Bundesregierung hat die Kritik aus der Entscheidung bereits aufgenommen und im Entwurf eines Änderungsgesetzes zum BDSG § 31 gestrichen und dafür einen neuen § 37a aufgenommen, der Erlaubnistatbestände im Sinn des Art. 22 Abs. 2 Buchst. b DS-GVO enthält. Damit wäre das Scoring als automatisierte Entscheidung erlaubt.

Während dadurch die Entscheidung des EuGH im Ergebnis für die Tätigkeit der Auskunfteien keine großen Auswirkungen hat, dürfte sie für alle Entscheidungsunterstützungssysteme – insbesondere für den Einsatz von Systemen der Künstlichen Intelligenz – noch von großer Bedeutung sein.

Über die Autoren

Prof. Dr. Alexander Roßnagel
ist Hessischer Beauftragter für Datenschutz und Informationsfreiheit. Zuvor war er Seniorprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel.

Maria Christina Rost
ist Ministerialrätin beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI).

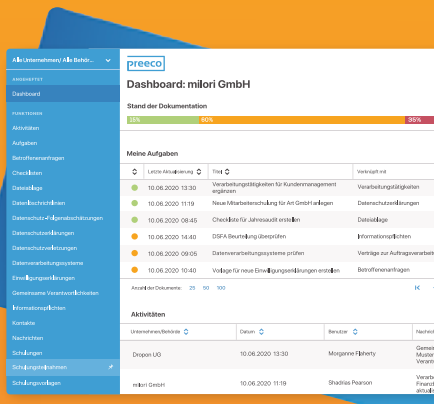
▶ https://datenschutz.hessen.de/

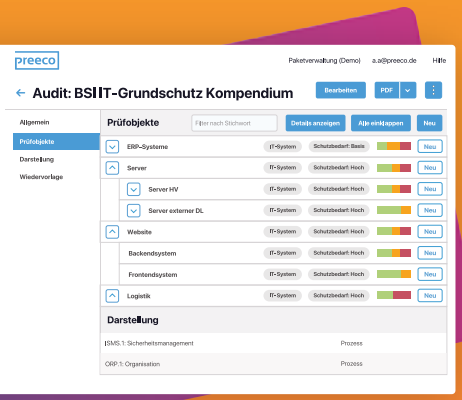
Anzeige

Smarte Software für Sie!

Datenschutz

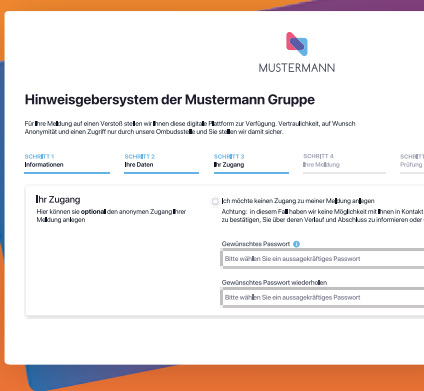
Unterstützt interne und externe Datenschutz-Teams.
Schafft Strukturen, spart Zeit.





Informationssicherheit

Unterstützt interne und externe Teams der Informationssicherheit.
Sicherheitsgewinn durch Transparenz.



Hinweisgeberschutz

Unterstützt interne und externe Ombudspersonen.
Vertraulich mit Hinweisgebenden kommunizieren.

Jetzt internen Meldekanal umsetzen ab 69,– € im Monat

preeco

+49 731 280 6510 sales@preeco.de www.preeco.de/bvd

AKTUELLES ZU SCHADENSERSATZ-ANSPRÜCHEN NACH CYBER-ANGRIFFEN

DR. PATRICK GROSMANN, DR. CHRISTOPH BAUSEWEIN

Die drei Türme des EuGH (von links nach rechts): Rocca, Montesquieu und Comenius (Foto: Gerichtshof der Europäischen Union)

Beweisanforderungen an immateriellen Schaden im Sinne der DSGVO und die Geeignetheit von technischen und organisatorischen Maßnahmen (TOM)

Cyberangriffe treffen nicht nur eine Vielzahl von Behörden und Unternehmen, sondern beschäftigen auch die Gerichte – bis hin zum Europäischen Gerichtshof (EuGH). Neben dem enormen wirtschaftlichen Schaden, der oftmals aus Cyberangriffen resultiert, sehen sich Verantwortliche immer wieder Haftungsprozessen ausgesetzt. Die Haftungsprozesse können entweder behördliche Bußgelder wegen Datenschutzverstößen oder Schadensersatzprozesse von Betroffenen betreffen. Zur Geltendmachung von Schadensersatzansprüchen hat der EuGH im Dezember 2023 (EuGH, Urt. v. 14.12.2023 – C-340/21) wesentliche Klarstellungen getroffen, die im Folgenden beleuchtet werden sollen.

1. Kernaussagen des EuGH

Unter Anerkennung, dass es nach dem Willen des Unionsgesetzgebers keine absolute Cybersicherheit geben kann, geht der EuGH davon aus, dass es für Verantwortliche nach der DSGVO lediglich die Pflicht gibt Datenschutzverletzungen beziehungsweise Cyberangriffe einzudämmen (EuGH, Urt. v. 14.12.2023 – C-340/21, Rn. 38). Losgelöst davon ist der Verantwortliche schadenersatzpflichtig, wenn infolge eines Cyberangriffs personenbezogene Daten abhandengekommen sind und missbräuchlich genutzt werden. Es sei denn, der Verantwortliche kann nachweisen, dass die von ihm getroffenen TOM angemessen waren. Ein Cyberangriff führt dementsprechend nach der Rechtsprechung des EuGH nicht automatisch zu einem Beweis der Ungeeignetheit der TOM.

2. Sachverhalt

Die Entscheidung des EuGH betrifft einen Cyberangriff auf die bulgarische Finanzbehörde. In dessen Folge wurden durch diverse Betroffene Forderungen auf immateriellen Schadensersatz geltend gemacht. Begründet wurde der Schadensersatzanspruch mit der Befürchtung, dass entwendete Daten in Zukunft möglicherweise missbräuchlich genutzt, im Internet veröffentlicht oder als Druckmittel gegen die Betroffenen verwendet werden könnten.

3. Entscheidung des Gerichts

Kein Beweis ungeeigneter TOM durch einen Cyberangriff

Das Urteil des EuGH beginnt mit der Feststellung, dass alleine durch einen *(erfolgreichen)* Cyberangriff die Ungeeignetheit von TOM nicht bewiesen ist. Aus dem Umstand eines (erfolgreichen)

Cyberangriffs kann also nicht ohne Weiteres geschlossen werden, dass der Verantwortliche keine geeigneten TOM getroffen hatte (Art. 24 Abs. 1 S. 1, 32 DSGVO).

Unter anderem aus der in der DSGVO fest verankerten Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) folgert das Gericht, dass dem Verantwortlichen die Möglichkeit bleiben muss die Geeignetheit seiner TOM beweisen zu können. Zudem ergibt sich für das Gericht aus dem risikobasierten Ansatz[1] der DSGVO ein Argument dafür, dass der Verantwortliche nie einen absoluten Schutz gewährleisten kann – und dies daher dem Verantwortlichen bei einem Cyberangriff auch nicht entgegengehalten werden kann.

Geeignetheit von TOM, abhängig vom Risiko

Weiter bestätigt der EuGH in seinem Urteil, dass sich die Geeignetheit der TOM nach der jeweils konkreten Verarbeitungstätigkeit richtet. Je riskanter eine Verarbeitungstätigkeit und sensibler die verarbeiteten Daten, desto höher sind die Anforderungen an die jeweiligen TOM. Hauptaufgabe des Verantwortlichen ist: Die Risiken für die Betroffenen müssen so weit wie möglich reduziert werden – Stichwort *Risikovermeidung*.

Als konkrete Hilfestellung für Praktiker sieht der EuGH eine Prüfung der Geeignetheit der TOM in zwei Schritten vor:

1. Bestimmung der konkreten Risiken[2] der jeweiligen Verarbeitungstätigkeit für Betroffene.
2. Festlegung angemessener TOM *unter Berücksichtigung des Risikos, des Stands der Technik,[3] der (dem jeweiligen Verantwortlichen gemessen an seiner Grö ße und Leistungsfähigkeit zumutbaren[4]) Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung* (siehe Art. 32 Abs. 1 DSGVO).

Beweislastumkehr bei Schadenersatzforderungen

Der EuGH leitet aus dem Wortlaut des Art. 5 Abs. 2 DSGVO (Rechenschaftspflicht) des Art. 24 Abs. 1 DSGVO (Verantwortung für die Datenverarbeitung) und des Art. 32 Abs. 1 DSGVO (TOM) ab, dass der Verantwortliche die Beweislast für die Geeignetheit der TOM trägt. Bei der Geltendmachung eines immateriellen Schadensersatzes durch Betroffene führt dies zu einer Beweislastumkehr zulasten des Verantwortlichen: Wird ein Verantwortlicher auf (immateriellen) Schadensersatz in Anspruch genommen, muss dieser stets beweisen, dass die TOM geeignet, also für die konkrete Verarbeitung ausreichend waren.

Die Beweislastumkehr stützt der EuGH vor allem auf zwei Argumente: Die Wertungen der DSGVO legen nach Auffassung des Gerichts nahe, dass der Verantwortliche durch seine Schutzmaßnahmen das Risiko für die Betroffenen weitgehend reduzieren muss. Die Möglichkeiten der Betroffenen einen (immateriellen) Schadensersatz gegenüber einem Verantwortlichen geltend zu machen, sähe das Gericht unverhältnismäßig eingeschränkt, wenn Betroffenen beweisen müssten, dass die TOM des Verantwortlichen ungeeignet waren, was sie mangels Einblicks in die Verarbeitungsvorgänge und ein umfassendes technisches Wissen der Betroffenen regelmäßig nicht leisten können.

Haftung des Verantwortlichen auch für eine Offenlegung von Daten durch Dritte

Wenn es bei Cyberangriffen zu einer Offenlegung von Daten kommt (sog. Data-Leaks), erfolgt dies nicht durch den Verantwortlichen selbst, sondern durch Hacker, also durch Dritte. Nach der Auffassung des EuGH führt dieser Umstand (Offenlegung durch Dritte) jedoch nicht dazu, dass der Verantwortliche (durch den nicht unmittelbar das Leaken der Daten erfolgte) von dessen Haftung befreit wird. Es bleibt also dabei, dass dem Verantwortlichen die Datenschutzverletzung nur dann zugerechnet werden kann, wenn dieser die Verletzung, unter Missachtung einer Verpflichtung aus der DSGVO, ermöglicht hat.

Schaden durch Befürchtung einer missbräuchlichen Nutzung

Hinsichtlich der Anforderungen an einen immateriellen Schaden bleibt die Entscheidung vage: Der EuGH geht zwar davon aus, dass bereits aus der bloßen Befürchtung einer (zukünftigen) missbräuchlichen Nutzung der personenbezogenen Daten ein immaterieller Schaden resultieren kann. Welche konkreten Anforderungen an den Beweis eines solchen immateriellen Schadens seitens des Betroffenen zu stellen sind, lässt das Gericht jedoch offen. Ungeklärt bleibt somit, wie ein Betroffener einen immateriellen Schaden (etwa die Befürchtung einer missbräuchlichen Nutzung) konkret beweisen muss. Die Beweislast dafür liegt in jedem Fall beim Betroffenen.

Dass bereits die bloße Befürchtung einer missbräuchlichen Nutzung für einen immateriellen Schaden genügt, schließt der EuGH aus dem Wortlaut des Art. 82 Abs. 1 DSGVO. Eine Unterscheidung zwischen einer bereits erfolgten missbräuchlichen Nutzung und der bloßen Angst davor, erkennt das Gericht darin nicht.

[1] Dieser findet in der DSGVO an unterschiedlichen Stellen seinen Niederschlag. Neben den TOM, wird dieser auch im Zusammenhang der Aufgabenzuschreibung des Datenschutzbeauftragten (Art. 39 Abs. 2 DSGVO) und der Datenschutz-Folgenabschätzung (Art. 35 DSGVO) zugrunde gelegt.

[2] Dies meint ein Risiko iSd ErwG 75 der DSGVO.

[3] Hierbei handelt es sich um einen unbestimmten Rechtsbegriff, der nach den bewährten Methoden auszulegen ist. Hilfestellung kann hierbei etwa die Handreichung zum Stand der Technik des Bundesverband IT-Sicherheit e.V. (TeleTrust) geben, in der englischen Fassung in Kooperation mit der Agentur der Europäischen Union für Cybersicherheit (ENISA), https://www.teletrust.de/publikationen/broschueren/stand-der-technik/.

[4] Martini, in Paal/Pauly/ 3. Aufl. 2021, Art. 32 DSGVO, Rn. 60.

4. Konsequenzen des EuGH-Urteils für die Praxis

Der Auswahl und Implementierung angemessener TOM kommt mehr denn je eine große Bedeutung zu. Die TOM müssen sich stets individuell an den jeweiligen Verarbeitungstätigkeiten orientieren. Für die Praxis bedeutet dies Folgendes: Zur Reduzierung finanzieller Risiken im Zusammenhang mit Cyberangriffen durch individuelle Schadenersatzforderungen von Betroffenen müssen Verantwortliche sich in einem ersten Schritt ernsthaft und sorgfältig mit der Bestimmung der individuellen Risiken befassen. Daran orientiert müssen Verantwortliche im zweiten Schritt passende TOM ergreifen. Hierbei wird es von entscheidender Bedeutung sein, dass sich der Verantwortliche bewusst ist, welche personenbezogenen Daten wie verarbeitet werden. Verantwortliche, die umfassende Verarbeitungsverzeichnisse führen, sind hier klar im Vorteil.

Infolge des EuGH-Urteils kann es für Verantwortliche mehr denn je sinnvoll sein sich nach anerkannten Standards, mit denen gewisse TOM und korrespondierende Kontrollen einhergehen, durch unabhängige Dritte (etwa nach dem ISO-Standard 27001:2022) zertifizieren zu lassen. So lässt sich im Ernstfall einfacher beweisen, dass die TOM geeignet waren. Dasselbe gilt mit Blick auf die Durchführung und Dokumentation von in regelmäßigen Abständen stattfindenden Cyber-Sicherheit-Checks[5] oder Überprüfungen[6] des eigenen Betriebs durch einen qualifizierten und unabhängigen Dritten. Für Verantwortliche empfiehlt sich zudem stets eine sorgfältige Dokumentation des Prozesses – nicht nur zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

Ebenso wichtig sind regelmäßige Datenschutz-Audits durch den Datenschutzbeauftragten. Die Entscheidung des EuGH verdeutlicht dabei, wie wichtig ein starker technischer Fokus bei der Durchführung der Audits ist: Sofern der Datenschutzbeauftragte nicht selbst über das erforderliche technische Knowhow verfügt, sollte er sich fachkundige Unterstützung holen (etwa durch den IT-Sicherheitsbeauftragten).

Die konkrete Bestimmung geeigneter TOM fällt in der Praxis oftmals schwer: Neben Regelungen zur IT-Sicherheit (z.B. BSI Grundschutz) kann auch die Handreichung zum Stand der Technik des Bundesverband IT-Sicherheit e.V. (TeleTrust) Hilfestellungen bieten. Der Vorteil dieser Orientierungshilfe liegt darin, dass sie von einer Institution der Europäischen Union (EU), der Agentur der Europäischen Union für Cybersicherheit (ENISA), anerkannt ist und sogar in der englischen Fassung von dieser mitherausgegeben wird.

Ähnlich nützliche Hilfestellung vermag auch ein kürzlich von der schweizerischen Datenschutz-Aufsichtsbehörde, dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), veröffentlichter Leitfaden zu TOM liefern.[7] Wenn auch außerhalb des Anwendungsbereichs der DSGVO, enthält dieser einige gute Anhaltspunkte, welche Schutzmaßnahmen gegenwärtig als angemessen angesehen werden können.

Konkrete Anforderungen an die TOM können sich in der Praxis auch aus branchenspezifischen Regelungen, etwa der IT-Sicherheitsrichtlinie der Kassenärztlichen Bundesvereinigung für kassenärztliche Arztpraxen ergeben.[8] Bei der Bestimmung der geeigneten TOM können solche bereichsspezifischen Regelungen nicht außer Acht gelassen werden. Mit Blick auf die möglichen Kosten einer Massenklage lässt sich infolge des EuGH-Urteils eine Investition in die TOM besser denn je rechtfertigen: In dem Ausgangsverfahren waren laut Medienberichten ca. 6 Mio. Personen von dem Cyberangriff betroffen. Die Klägerin des Ausgangverfahrens machte Schadensersatz in Höhe von ca. 510,- Euro gegen die Verantwortlichen geltend. Wenn nur ein Bruchteil der Betroffenen einen Schadensersatz in dieser Höhe geltend macht, führt dies zu einem enormen finanziellen Risiko.

5. Auswirkungen für die deutsche Rechtsprechung

Neben diesen für die Praxis äußerst relevanten Klärungen verbleiben auch nach der Entscheidung des EuGH Unklarheiten bezüglich der Anforderungen für die Geltendmachung eines immateriellen Schadensersatzanspruchs vor nationalen Gerichten. Insbesondere bleibt unklar, wie ein immaterieller Schaden aufgrund der bloßen Befürchtung einer missbräuchlichen Nutzung personenbezogener Daten zu begründen und schlussendlich zu beweisen ist. Dies muss durch die nationalen Gerichte noch definiert werden. Aktuell zeichnet sich im Lichte der in jüngerer Vergangenheit ergangener Gerichtsentscheidungen in Deutschland folgendes Bild: Erforderlich bleiben konkrete Angaben zu den individuellen Auswirkungen auf die jeweilige betroffene Person.[9]

[5] Dazu wurde vom ISACA Germany Chapter e. V. ein gleichnamiger Leitfaden zuletzt im Jahre 2020 veröffentlicht, der Anleitung zur Vorgehensweise gibt: https://www.isaca.de/images/Publikationen/Leitfaden/Leitfaden_Cyber-Sicherheits-Check_V2.pdf.

[6] Folgende Überprüfungen kommen dabei in Frage: Response Readiness Exercise, Soc Assessment, Cybersecurity Maturity Assessment, Cybersecurity Program Semi-Annual Review, Security Program In-Depth Assessment, Ransomware Defense Assessment, Cybersecurity Technical Tabletop Exercise, Executive Briefings, Compromise Assessment. Technical Risk Assessment, Cyber Threat Risk Evaluation, Cloud Security Assessment, Cloud Compromise Assessment, Identity Security Assessment.

[7] Siehe unter: https://www.edoeb.admin.ch/edoeb/de/home/kurzmeldungen/km2024/23012024_leitfaden_tom.html.

[8] Siehe dazu: https://www.kbv.de/html/it-sicherheit.php.

[9] Das OLG Stuttgart stellte in diesem Zusammenhang fest: „im Einzelfall ist es deshalb ausreichend, aber auch erforderlich, dass der Betroffene Umstände darlegt, in denen sich seine erlebten Empfindungen widerspiegeln, und dass nach der Lebenserfahrung der Datenschutzverstoß mit seinen Folgen Einfluss auf das subjektive Empfinden hat“, OLG Stuttgart, Urt. v. 22.11.2023 – 4 U 20/23, in GRUR-RS 2023, 32883, Rn. 295.

"Massenklagen" sind daher in der Praxis zunächst nur eingeschränkt umsetzbar.

So hat unter anderem das OLG Hamm im Dezember 2023 entschieden, dass bei dem sog. Scraping[10] von Daten von einem Facebook-Account im Einzelfall zu beweisen ist, worin der immaterielle Schaden der betroffenen Person liegt (OLG Hamm, Beschl. v. 21.12.2023 – 7 U 137/23).

In einer anderen Entscheidung zu Saturn hat der EuGH im Januar 2024 entschieden, dass die bloße versehentliche Veröffentlichung personenbezogener Daten, ohne dass diese von einem Dritten zur Kenntnis genommen wurden, keinen immateriellen Schaden begründet (EuGH, Urt. v. 25.01.2024 – C-687/21).

FAZIT

Jeder Verantwortliche (und jeder Datenschutzbeauftragte) sollte sich regelmäßig und intensiv damit beschäftigen, ob die TOM geeignet sind und dem Stand der Technik entsprechen. Wurde der Verantwortliche erst einmal zum Opfer eines Cyberangriffs, ist es dafür bereits zu spät. Regelmäßige Datenschutz-Audits durch den Datenschutzbeauftragten und unabhängige Dritte können aufzeigen, an welchen Stellen die TOM lückenhaft sind. Gleichzeitig ist eine gute Dokumentation der TOM sinnvoll, da sich Verantwortliche damit gegen Schadensersatzforderungen von Betroffenen verteidigen können.

[10] Scraping ist das meist automatisierte Abgreifen fremder Inhalte im Internet.

Über die Autoren

Dr. Patrick Grosmann, M.A.
Rechtsanwalt der Kanzlei FPS PartG mbB in Frankfurt. Zert. Datenschutzbeauftragter (TÜV®) und Datenschutz-Auditor (DGI®), Promotion zu Interessenkonflikten der Datenschutzbeauftragten, Dozent für Datenschutzbeauftragte. Er berät im IT- & Datenschutzrecht.

Dr. Christoph Bausewein
CIPP/E | CIPT
BvD Vorstand, Assistant General Counsel, Data Protection & Policy bei der US-Cybersicherheitsfirma CrowdStrike, Mitglied des Expertenrats des Europäischen Datenschutzausschuss (EDSA) für neue Technologien.

Anzeige

Für interne & externe Datenschutzbeauftragte

Sie suchen eine Haftpflicht-Versicherung?
Sie möchten Ihre bestehende Police vergleichen?

Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.

Berufs-Haftpflichtversicherung für interne und externe DSB – in Zusammenarbeit mit dem BvD entwickelt:

- exklusives Wording (eDSB und erweiterte Tätigkeiten im Datenschutz mitversichert)
- optional inkl. Unternehmensberater, Informationssicherheits-Beauftragter
- niedrige Prämien & professionelle Beratung
- nähere Informationen auch unter www.bvdnet.de (Mitgliederbereich)

NEU:

- **Tätigkeit der Hinweisgebermeldestelle ist beitragsfrei mitversichert**
- **Leistungs-Update**
- **Jahreshöchstleistung: das 4-fache der Versicherungssumme**

BUTZ VERSICHERUNGSMAKLER GMBH

Ansprechpartner: Herr Jared Butz
Tel: 0 6174 - 96 843 - 0
Mail: info@butz-versicherungsmakler.de
www.butz-versicherungsmakler.de

DR. BERND SCHÜTZE

VERARBEITUNG VON IN ART. 9 ABS. 1 DS-GVO GENANNTEN DATENKATEGORIEN

Auswirkungen des EuGH-Urteils zum Umgang mit Erlaubnistatbeständen

Entsprechend des Urteils des Gerichtshofs der Europäischen Union (EuGH) ist für die Verarbeitung von Daten, welche zu den in Art. 9 Abs. 1 DS-GVO genannten Kategorien zählen, sowohl ein Erlaubnistatbestand gem. Art. 9 Abs. 2 DS-GVO erforderlich, aber ergänzend müssen die in Art. 6 Abs. 1 DS-GVO genannten Rechtmäßigkeitsvoraussetzungen erfüllt sein.[1]

Hierbei ist zu beachten, dass entsprechend der Rechtsprechung des EuGH die Zuordnung eines Datums als „sensibles Datum" i.S. d. Art. 9 Abs, 1 DS-GVO weit zu verstehen ist[2]. Weiterhin urteilte der EuGH, dass ein Datensatz, der sowohl sensible als auch nicht sensible Daten enthält, insgesamt als sensibles Datum i. S. v. Art. 9 Abs. 1 DS-GVO anzusehen ist.[3]

Hinsichtlich der in Art. 6 Abs. 1 und Art. 9 Abs. 2 DS-GVO genannten Erlaubnistatbestände urteilte der EuGH[4,5], dass die Erlaubnistatbestände eng auszulegen sind, da die dort genannten Rechtfertigungsgründe dazu führen können, dass eine Verarbeitung personenbezogener Daten trotz fehlender Einwilligung der betroffenen Person rechtmäßig ist.

Somit muss beachtet werden, dass zusätzlich zu den in Art. 9 Abs. 2 DS-GVO genannten Tatbestände mindestens einer der in Art. 6 Abs. 1 DS-GVO genannten Anforderungen erfüllt wird. Im Folgenden erfolgt daher eine Betrachtung, welche der in Art. 9 und Art. 6 DS-GVO genannten Rechtfertigungsgründe für eine Verarbeitung personenbezogener Daten miteinander in Beziehung gebracht werden könnten.

Art. 9 Abs. 2 lit. a DS-GVO

Art. 9 Abs. 2 lit. a DS-GVO beinhaltet die ausdrückliche Einwilligung, hier wird direkt Art. 6 Abs. 1 lit. a ebenfalls erfüllt. Erwähnenswert in diesem Zusammenhang ist ein anderes Urteil des EuGH[6]: Der Verantwortliche muss nachweisen (können), dass betroffene Personen ihre jeweilige Einwilligung durch aktives Verhalten bekundet haben und zuvor Information über alle Umstände im Zusammenhang mit der Verarbeitung erhielten, welcher der jeweiligen Person erlaubten die Konsequenzen dieser Einwilligung leicht zu ermitteln, sodass gewährleistet ist, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird.

Zu beachten: Es können auch mehrere Tatbestände aus Art. 6 Abs. 1 DS-GVO zutreffen. Wenn beispielsweise ein App-Hersteller sensible personenbezogene Daten – wie z. B. Gesundheitsdaten (Puls, Schrittzahl usw.) durch Fitness-Apps – verarbeitet, so kann nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO diese Verarbeitung legitimieren (siehe auch in Abschnitt Art. 9 Abs. 2 lit. h DS-GVO die Hinweise zu einem Vertrag mit einem Angehörigen eines Gesundheitsberufs). Als Rechtfertigungsgrund aus Art. 6 Abs. 1 DS-GVO treffen sowohl Art. 6 Abs. 1 lit. a DS-GVO (Einwilligung) aber ggf. auch Art. 6 Abs. 1 lit. b DS-GVO (Vertragserfüllung) zu.

Wie es im Urteil des EuGH in Leitsatz 3 zu finden ist, muss „mindestens eine der in Art. 6 Abs. 1 genannten Recht-

[1] EuGH, Urt. v. 2023-12-21, Rechtssache C-667/21, Rn. 79. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0667

[2] EuGH, Urt. v. 2022-08-01, Rechtssache C-92/09, C-93/09, Rn. 119, 120, 125. Online, zitiert am 2023-12-29; verfügbar unter https://dejure.org/2010,236 bzw. Volltext abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1698904362512&uri=CELEX%3A62020CJ0184

[3] EuGH, Urt. v. 20263-07-04, Rechtssache C-252/21, Rn. 89 sowie Leitsatz 2. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252

[4] EuGH, Urt. v-2023-07-04, Rechtssache C-252/21, Rn. 76. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252

[5] EuGH, Urt. v-2023-07-04, Rechtssache C-252/21, Rn. 93. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252

[6] EuGH Urt. v. 2021-01-18, Rechtssache C-61/19, zu finden im Tenor des Urteils. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62019CA0061&qid=1703360472835

Die große Kammer des EugH. Foto: Gerichtshof der Europäischen Union

mäßigkeitsvoraussetzungen erfüllt werden; es können aber auch mehrere erfüllt werden.

Art. 9 Abs. 2 lit. b DS-GVO

Art. 9 Abs. 2 lit. b DS-GVO erlaubt die Verarbeitung, sofern diese erforderlich ist, damit der „Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen“ können. Pflichten aus dem Arbeitsrecht können einerseits aus nationalen Gesetzen resultieren, aber auch aus einem Arbeitsvertrag, korrespondierende Tatbestände wären dementsprechend Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) oder Art. 6 Abs. 1 lit. c DS-GVO (zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt).

Bzgl. dem zweiten Teil von Art. 9 Abs. 2 lit. b DS-GVO (Recht der sozialen Sicherheit und des Sozialschutzes) finden sich die gesetzlichen Regelungen in den deutschen Sozialgesetzbüchern, somit wird hier ebenfalls Art. 6 Abs. 1 lit. c DS-GVO (zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt) entsprochen.

Hinsichtlich Art. 6 Abs. 1 lit. c DS-GVO ist darauf hinzuweisen, dass die Regelung ausschließlich Verpflichtungen kraft objektiven Rechts adressiert, jedoch keine gesetzlich geregelten Möglichkeiten, um personenbezogene Daten zu verarbeiten. Im deutschen Recht finden sich beispielsweise diverse Verpflichtungen zur Speicherung und Übermittlung von Daten, z. B. im Steuer- oder Telekommunikationsrecht. Gesetzliche Erlaubnistatbestände, Daten zu verarbeiten, wenn der Verantwortliche dies möchte, fallen hingegen nicht darunter; ohne eine Pflicht zur Verarbeitung für den Verantwortlichen ist die Bedingung der Erforderlichkeit nicht erfüllt.[7] Somit finden gesetzliche Regelungen, welche die Verarbeitung z. B. für wissenschaftliche oder historische Forschungszwecke sowie statistische Zwecke erlauben, keine Entsprechung in Art. 6 Abs. 1 lit. c DS-GVO. D. h., in diesen Fällen muss ein anderer Rechtfertigungstatbestand aus Art. 6 Abs. 1 DS-GVO gefunden werden.

Art. 9 Abs. 2 lit. c DS-GVO

Art. 9 Abs. 2 lit. c DS-GVO gestattet die Verarbeitung im erforderlichen Umfang zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person, sofern die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben. Diese Regelung findet ihre Entsprechung in Art. 6 Abs. lit. d DS-GVO, sodass mit Art. 9 Abs. 2 lit. c DS-GVO zugleich auch Art. 6 Abs. 1 lit. d DS-GVO eingehalten wird.

[7] So z. B.:
- Buchner B, Petri T.: Art. 6, Rn. 77. In: Kühling / Buchner (Hrsg.) Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. C. H. Beck, 3. Auflage 2020. ISBN: 978-3-406-74994-0
- Kremer P.: Art. 6. Rn. 53. In: Eßer / Kramer / von Lewinski (Hrsg.) DSGVO / BDSG: Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze (Auernhammer). Wolters Kluwer, 7. Auflage 2020. ISBN 978-3-452-295-26-2
- Roßnagel A.: Art. 6, Rn. 57. In: Simitis / Hornung / Spiecker gen. Döhmann (Hrsg.) Datenschutzrecht. Nomos, 1. Auflage 2019. ISBN 978-3-8487-3590-7

Art. 9 Abs. 2 lit. d DS-GVO

Art. 9 Abs. 2 lit. d DS-GVO erlaubt eine Verarbeitung auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten, jedoch nur, wenn sich die Verarbeitung

a) ausschließlich auf die Mitglieder oder

b) ehemalige Mitglieder der Organisation oder

c) auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten,

bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden.

Hierzu findet sich keine direkte Entsprechung in Art. 6 Abs. 1 DS-GVO. Bzgl. Mitgliedern oder ehemaligen Mitgliedern kann – sofern ein Vertrag bzgl. Mitgliedschaft in der jeweiligen Organisation oder auch eine Satzung entsprechendes berücksichtigt – Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) herangezogen werden. Dies gilt jedoch nicht für Personen, die lediglich Kontakte mit der jeweiligen Organisation unterhalten bzw. unterhielten. Hier wird i. d. R. Art. 6 Abs. 1 lit. f DS-GVO herangezogen werden müssen und im Rahmen einer Interessensabwägung geprüft werden, ob eine Verarbeitung statthaft ist.

Entsprechend ErwGr. 47 DS-GVO stellt ein Faktor, der bei jeder Interessensabwägung berücksichtigt werden muss, die „vernünftigen Erwartungen" der betroffenen Person dar, die auf der Beziehung der Person zu dem Verantwortlichen beruhen. Ein weiterer zu beachtender Punkt liegt nach ErwGr. 47 DS-GVO in dem Umstand, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Laut ErwGr 47 DS-GVO können die Interessen der betroffenen Person insbesondere dann überwiegen, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss. Und je sensibler die zu verarbeitenden Daten, desto schwerer ist gemäß der Rechtsprechung des EuGH[8] der Eingriff in die in den Art. 7 und 8 der Charta verankerten Grundrechte der betroffenen Person, sodass auch die Sensibilität der Daten im Rahmen einer Interessensabwägung zu berücksichtigen ist; bei Art. 9 Abs. 2 lit. d DS-GVO handelt es sich naturgemäß um Daten der besonders schützenswerten Kategorien, entsprechend sind die Interessen betroffener Personen zu berücksichtigen.

Art. 9 Abs. 2 lit. e DS-GVO

Der Tatbestand in Art. 9 Abs. 2 lit. e DS-GVO betrifft Verarbeitung von personenbezogenen Daten, welche die betroffene Person offensichtlich öffentlich gemacht hat. Auch hier findet sich keine entsprechende Regelung in Art. 6 Abs. 1 DS-GVO, sodass auch in diesen Fällen i. d. R. eine Interessensabwägung gemäß Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein wird; auf die in Abschnitt Art. 9 Abs. 2 lit. d DS-GVO gegebenen Hinweise zur Interessensabwägung wird hingewiesen.

Art. 9 Abs. 2 lit. f DS-GVO

Art. 9 Abs. 2 lit. f DS-GVO gestattet die Verarbeitung im erforderlichen Umfang zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit. In den meisten Fällen, wo diese Regelung angewandt wird, wird auch Art. 6 Abs. 1 lit. c DS-GVO (zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt) zutreffen: Grundsätzlich prägt einen Zivilprozess der Beibringungsgrundsatz, jedoch verpflichtet § 139 Abs. 1 S. 2 ZPO das Gericht die beteiligten Parteien zur Mitwirkung an der Aufklärung des Sachverhalts sowie zur Beibringung von fehlenden Informationen zu bewegen. Unterliegt der Verantwortliche einer entsprechenden Mitwirkungspflicht, so ist Art. 6 Abs. 1 lit. c DS-GVO anwendbar.

Eine Sitzung in der Kammer mit fünf Richtern (Foto: Gerichtshof der Europäischen Union)

Beruht die Verarbeitung auf einem Vertrag entsprechend Art. 9 Abs. 2 lit. h DS-GVO, so ist natürlich auch Art. 6 Abs. 1 lit. b DS-GVO anwendbar.

Erfolgt die Verarbeitung hingegen eher vorsorglich, z. B. um Daten für ein möglicherweise in irgendeiner unbestimmten Zukunft anstehendes Gerichtsverfahren zu speichern, so wird sich keine gesetzliche Regelung finden, die dies vom

[8] EuGH Urt. v. 2023-12-07, Rechtssache C-26/22, C-64/22, Rn. 94. Online, zitiert am 2023-12-12; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0026

Verantwortlichen verlangt, somit ist ein rechtliches Erfordernis nicht gegeben. Auch in diesen Fällen wird eine Interessensabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein und eine Verarbeitung ist dann nur möglich, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; auf die in Abschnitt Art. 9 Abs. 2 lit. d DS-GVO gegebenen Hinweise zur Interessensabwägung wird wiederum hingewiesen.

Art. 9 Abs. 2 lit. g DS-GVO

Art. 9 Abs. 2 lit. g DS-GVO erlaubt eine Verarbeitung, wenn diese

a) aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist und

b) Unionsrecht oder deutsches Recht dies erlaubt, wobei diese gesetzliche Regelung

   1. in angemessenem Verhältnis zu dem verfolgten Ziel stehen,

   2. den Wesensgehalt des Rechts auf Datenschutz wahren und

   3. angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen muss.

Der Verantwortliche muss also diese Vorgaben prüfen, bevor Art. 9 Abs. 2 lit. g DS-GVO überhaupt angewendet werden kann. Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) wird durch Art. 9 Abs. 2 lit. g DS-GVO i. d. R. ebenfalls entsprochen.

Art. 9 Abs. 2 lit. h DS-GVO

Art. 9 Abs. 2 lit. h DS-GVO beinhaltet diverse Zwecke und erlaubt eine Verarbeitung im erforderlichen Umfang für Zwecke

a) der Gesundheitsvorsorge,

b) der Arbeitsmedizin,

c) der Beurteilung der Arbeitsfähigkeit des Beschäftigten,

d) der medizinischen Diagnostik,

e) der Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder

f) der Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich,

wobei entweder Unionsrecht oder deutsches Recht die konkrete Erlaubnisnorm beinhalten müssen oder ein Vertrag mit einem Angehörigen eines Gesundheitsberufes vorliegen muss.

Im deutschen Recht finden sich hier diverse Regelungen, welche dies adressieren: im Bundesrecht z. B. die Sozialgesetzbücher, im Landesrecht beispielsweise die Rettungsdienstgesetze der Länder oder Landeskrankenhausgesetze.

Hinsichtlich vertraglicher Regelung ist in Deutschland insbesondere auf den in §§ 630a ff BGB geregelten Behandlungsvertrag hinzuweisen.

Zu beachten bei der in Art. 9 Abs. 2 lit. h DS-GVO enthaltenen vertraglichen Rechtsgrundlage ist die Forderung, dass der Vertrag mit „Angehörigen eines Gesundheitsberufs“ abgeschlossen sein muss. Der Terminus „Angehörige eines Gesundheitsberufs“ ist europarechtlich in Art. 3 lit. f Richtlinie 2011/24/EU[9] geregelt:

„Einen Arzt, eine Krankenschwester oder einen Krankenpfleger für allgemeine Pflege, einen Zahnarzt, eine Hebamme oder einen Apotheker im Sinne der Richtlinie 2005/36/EG oder eine andere Fachkraft, die im Gesundheitsbereich Tätigkeiten ausübt, die einem reglementierten Beruf im Sinne von Artikel 3 Absatz 1 Buchstabe a der Richtlinie 2005/36/EG[10] vorbehalten sind, oder eine Person, die nach den Rechtsvorschriften des Behandlungsmitgliedstaats als Angehöriger der Gesundheitsberufe gilt.“

In Deutschland dürften „Angehörigen eines Gesundheitsberufs“ weitestgehend mit jenen Berufen übereinstimmen, welche von § 203 Abs. 1 Ziff. 1 StGB adressiert werden: „Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert“.[11]

Somit werden Verträge mit Ärzten, Krankenpflegepersonal usw. wohl mit der Regelung in Art. 9 Abs. 2 lit. h DS-GVO adressiert, Verträge mit anderen Dienstleistern (z. B. zur Terminvermittlung zwischen einem Patienten und einem niedergelassenen Arzt, was entsprechend der weiten Auslegung[2,3] des Art. 9 Abs. 1 DS-GVO ebenfalls eine Verarbeitung sensibler Daten darstellt) werden hierdurch wohl eher nicht legalisiert werden können; ein Vertrag zwischen

[9] Art. 3 lit. f Richtlinie 2011/24/EU. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02011L0024-20140101#tocId6

[10] Art. 3 Abs. 1 lit. a der Richtlinie 2005/36/EG verweist auf „reglementierte Berufe“, bei welchen die Aufnahme oder Ausübung oder eine der Arten der Ausübung direkt oder indirekt durch Rechts- und Verwaltungsvorschriften an den Besitz bestimmter Berufsqualifikationen gebunden ist. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:02005L0036-20231009#tocId25

[11] Ein Hinweis hierzu findet sich z. B. in Schütze B, Spyra G. (2018) Schweigepflicht und die Einbindung externer Kräfte: endlich geregelt. Online, zitiert am 2023-12-29; verfügbar unter https://gesundheitsdatenschutz.org/html/schweigepflicht_05.php

Verantwortlichen, der kein Angehöriger eines Gesundheitsberufes ist, und betroffenen Personen kann Art. 6 Abs. 1 lit. b DS-GVO genügen, jedoch nicht die Verarbeitung von Daten legitimieren, welche zu den in Art. 9 Abs. 1 DS-GVO genannten Kategorien zählen. I. d. R. wird hier nur eine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO die Verarbeitung legalisieren können.[12] Richtigerweise wird daher auch für digitale Pflegeanwendungen nach § 40a SGB XI („DiPA") und digitalen Gesundheitsanwendungen gemäß § 33a SGB V („DiGA") in den jeweiligen Verordnungen nur eine Einwilligung als Rechtsgrundlage akzeptiert.[13]

Je nach Anwendung des Art. 9 Abs. 2 lit. h DS-GVO finden sich verschiedene Regelungen in Art. 6 Abs. 1 DS-GVO. Basiert die Verarbeitung auf der Grundlage eines Vertrages mit einem Angehörigen eines Gesundheitsberufs, so wird Art. 6 Abs. 1 lit. b DS-GVO (Erfüllung vertraglicher Pflichten) ebenfalls erfüllt sein.

Erfolgt die Verarbeitung hingegen aufgrund einer der diversen gesetzlichen Regelungen in Deutschland, so wird wohl eher Art. 6 Abs. 1 lit. c DS-GVO (zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt) zutreffen.

Art. 9 Abs. 2 lit. i DS-GVO

Art. 9 Abs. 2 lit. i DS-GVO erlaubt die Verarbeitung, wenn diese aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich ist. Beispielhaft wird angegeben:

- Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder
- Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten.

Weiterhin muss entweder das Unionsrecht oder das deutsche Recht die Verarbeitung erlauben. Dieses Recht muss angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsehen, ansonsten genügt das Recht nicht den Anforderungen von Art. 9 Abs. 2 lit. i DS-GVO.

In diesen Fällen wird bei Vorliegen eines Erlaubnistatbestandes nach Art. 9 Abs. 2 lit. i DS-GVO häufig auch den Anforderungen von Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) genügt werden.

Hierbei ist jedoch zu beachten, dass Art. 6 Abs. 3 neben der Grundlage einer nationalen oder unionsrechtlichen Rechtsgrundlage verlangt, dass die Verarbeitung der personenbezogenen Daten erforderlich zur Erfüllung ist. D. h., ohne diese Verarbeitung kann die im öffentlichen Interesse liegende oder in Ausübung öffentlicher Gewalt erfolgende Aufgabe nicht erfüllt werden.

Art. 9 Abs. 2 lit. j DS-GVO

Art. 9 Abs. 2 lit. j DS-GVO erlaubt die Verarbeitung personenbezogener Daten für

- im öffentlichen Interesse liegende Archivzwecke,
- für wissenschaftliche oder historische Forschungszwecke oder
- für statistische Zwecke gemäß Art. 89 Abs. 1 DS-GVO.

Damit dieser Erlaubnistatbestand angewendet werden kann, muss entweder das Unionsrecht oder das deutsche Recht die jeweilige Verarbeitung erlauben, wobei dieses Recht

a) in angemessenem Verhältnis zu dem verfolgten Ziel stehen,

b) den Wesensgehalt des Rechts auf Datenschutz wahren und

c) angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person

vorsehen muss.

Die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke findet einen korrespondierenden Erlaubnistatbestand in Art. 6 Abs. 1 lit. e DS-GVO (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe); siehe hierzu auch die im Abschnitt Art. 9 Abs. 2 lit. i DS-GVO gegebenen Hinweise.

Dies kann, muss aber nicht, auch für wissenschaftliche oder historische Forschungszwecke sowie statistische Zwecke gelten, je nachdem, ob die Forschung/Statistik im öffent-

[12] Hierbei sollten die Ausführungen des EuGH bzgl. des Meta-Falles beachtet werden: EuGH, Urt. v. 2023-07-04, Rechtssache C-252/21. Rn. 140 ff, insbesondere Rn. 154. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252

[13] Siehe

-§ 5 Abs. 3 DiPAV: „[…] dürfen nur aufgrund einer Einwilligung nach Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 […] und ausschließlich zu den folgenden Zwecken verarbeitet werden […]". Online, zitiert am 2023-12-29; verfügbar unter https://www.gesetze-im-internet.de/dipav/__5.html

-§ 4 Abs. 2 DiGAV: „[…] dürfen personenbezogene Daten nur aufgrund einer Einwilligung der Versicherten nach Artikel 9 Absatz 2 Buchstabe a der Verordnung (EU) 2016/679 […] und ausschließlich zu den folgenden Zwecken verarbeitet werden […]". Online, zitiert am 2023-12-29; verfügbar unter https://www.gesetze-im-internet.de/digav/__4.html

lichen Interesse liegt oder nicht; der Verantwortliche muss nachweisen (können), dass öffentliche Interesse an der Forschung/Statistik vorhanden ist. Was regelhaft nicht alleine durch das Vorhandensein von öffentlichen (Förder-)Gelder erreicht werden kann; diese können wohl einen Hinweis auf öffentliches Interesse geben, aber nicht alleine als Nachweis dienen.

Liegen die wissenschaftlichen oder historischen Forschungszwecke bzw. die statistischen Zwecke nicht im (nachweisbaren) öffentlichen Interesse, wird in diesen Fällen i. d. R. eine Interessensabwägung entsprechend Art. 6 Abs. 1 lit. f DS-GVO erforderlich sein; auf die im Abschnitt Art. 9 Abs. 2 lit. d DS-GVO gegebenen Hinweise zur Interessensabwägung wird hingewiesen.

Art. 9 Abs. 4 DS-GVO

Entsprechend Art. 9 Abs. 4 DS-GVO können die Mitgliedstaaten für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten.

Hierbei ist der nationale Gesetzgeber allerdings nicht völlig frei, er muss sich an die Vorgaben der DS-GVO halten und darf das Schutzniveau nicht beliebig herabsenken. Weiterhin ist zu beachten, dass Art. 7 und 8 der Charta der Grundrechte der Europäischen Union nur eingeschränkt werden können, wenn entsprechende Einschränkungen gemäß Art. 52 Abs. 1 der Charta gesetzlich vorgesehen sind und den Wesensgehalt der Grundrechte sowie den Grundsatz der Verhältnismäßigkeit wahren[14]. Nach Rechtsprechung des EuGH dürfen Einschränkungen nur vorgenommen werden, wenn

1. sie erforderlich sind und
2. den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen.

Basierend auf diesen Vorgaben erlassene Einschränkungen müssen sich auf das absolut Notwendige beschränken, die den Eingriff enthaltende Regelung muss klare und präzise Regeln für die Tragweite und die Anwendung der betreffenden Maßnahme vorsehen und über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken ermöglichen.[15]

Es kann zu Recht bezweifelt werden, dass diverse vom deutschen Gesetzgeber erlassene Regelungen diesen Vorgaben entsprechen, insbesondere auch Regelungen aus jüngerer Zeit wie beispielsweise das „Gesetz zur verbesserten Nutzung von Gesundheitsdaten“ (Gesundheitsdatennutzungsgesetz, GDNG). Im letztgenannten Gesetz fehlen beispielsweise „klare und präzise Regeln für die Tragweite und die Anwendung“, welche betroffenen Personen einerseits aufklären, wer wann zu welchen genauen Zwecken (medizinische „Forschung“ ist keine präzise Angabe und auch nicht jede Forschung liegt im oder dient dem öffentlichen Interesse) ihre Daten verarbeiten darf, andererseits verfügen betroffene Personen über keine ausreichenden Garantien hinsichtlich Missbrauchsschutz, erfahren i. d. R. nicht einmal, welche (natürliche oder juristische) Person die persönlichen Daten zu welchen Zwecken verarbeitet. Entsprechende Kritik wurde von Fachleuten bereits geäußert.[16]

Ein Gesetz ist allerdings so lange rechtskräftig anwendbar, bis entweder der Gesetzgeber das jeweilige Gesetz änderte oder ein Gericht dieses Gesetz für rechtswidrig und nicht anwendbar erklärte. Bei aller vorhandenen Kritik sind die Gesetze bis zum Widerruf durch den Gesetzgeber selbst oder einem entsprechenden Gerichtsurteil also anwendbar. Im Falle der Erlaubnistatbestände zur Verarbeitung personenbezogener Daten entsteht für Verantwortliche ggf. jedoch ein Risiko: Erkennt ein Gericht die Unrechtmäßigkeit eines Gesetzes an, so konnte das Gesetz die Verarbeitung der Daten niemals legitimieren. Entsprechend Treu und Glauben kann der Verantwortliche für die unrechtmäßige Verarbeitung in der Vergangenheit zwar nicht belangt werden, aber aufgrund der Unrechtmäßigkeit müssen alle Daten gelöscht werden, ggf. sogar Verarbeitungsergebnisse, die ja nie hätten angefertigt werden dürfen. Im Bereich von Medizinprodukten kann dies beispielsweise dazu führen, dass diese aufgrund fehlender Datengrundlage und damit feh-

[14] So z. B. zu finden in:

- EuGH, Urt. v. 2020-07-06, Rechtssache C-311/18. Rn. 172 bis 175. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62018CJ0311
- EuGH, Urt. v. 2022-08-01, Rechtssache C-184/20. Rn. 70. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62020CJ0184

[15] So z. B. zu finden in:

- EuGH, Urt. v. 2020-07-06, Rechtssache C-311/18. Rn. 176. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62018CJ0311
- EuGH, Urt. v. 2021-06-22, Rechtssache C-439/19. Rn. 105. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2021%3A504

[16] Siehe stellvertretend: Weichert T. (2023-11-14) Stellungnahme GDNG. Online, zitiert am 2023-12-29; verfügbar unter https://www.netzwerk-datenschutzexpertise.de/dokument/medizinische-forschung-und-datenschutz bzw. pdf-Datei unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/2023_stn_gdng.pdf

Aufgrund des Urteils des EuGH bekommen Verantwortliche „Hausaufgaben“, z. B.:

- Die Rechtsgrundlagen müssen überarbeitet und neu geprüft werden.
- Informations- und Auskunftspflichten sind anzupassen. Unter Umständen müssen betroffene Personen hinsichtlich geänderter Rahmenbedingungen informiert werden, beispielsweise, weil diesen jetzt nach Art. 13 Abs. 1 lit. d bzw. Art. 14 Abs. 2 lit. b DS-GVO die berechtigten Interessen mitgeteilt werden müssen.
- Die Dokumentation wie beispielsweise das Verzeichnis der Verarbeitungstätigkeiten müssen angepasst werden.
- Ggf. müssen auch Prozesse überarbeitet werden, wenn beispielsweise im Risikomanagement auch die Bewertung einer Interessensabwägung beachtet werden muss.

lendem Wirknachweis wieder vom Markt genommen werden müssen. Somit muss ein Verantwortlicher jeweils selbst abschätzen, ob für die eigene Verarbeitung die ggf. rechtswidrige gesetzliche Grundlage genutzt werden soll oder ob aus Sicherheitsgründen ein anderer, rechtssicherer Erlaubnistatbestand vielleicht besser geeignet ist.

Unabhängig davon gilt: Alle nationalen Erlaubnistatbestände zur Verarbeitung von personenbezogenen Daten sind nur in Verbindung mit den Vorgaben aus Art. 6 Abs. 2 DS-GVO sowie bei Verarbeitung von personenbezogenen Daten der besonderen Kategorie ergänzend denen aus Art 9 Abs. 4 DS-GVO anwendbar. D. h. nationale Regelungen müssen entsprechend Art. 6 Abs. 2 DS-GVO „spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten“ – eine reine Wiederholung von Texten der DS-GVO entspricht nicht diesen Anforderungen.[17] Spezifischere Regelungen „müssen auf den Schutz der Rechte und Freiheiten […] hinsichtlich der Verarbeitung ihrer personenbezogenen Daten […] abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen“[14].

Erfüllen die nationalen Regelungen diese Anforderungen, d. h. stellen keine reinen Wiederholungen der DS-GVO dar, können diese Regelungen für die Zeitdauer ihrer Gültigkeit angewendet werden. Die Anwendbarkeit erfolgt dann „nationale Regelung i. V. m. Art. 9 Abs. 4 DS-GVO“, also z. B. die in § 27 BDSG zu findende Interessensabwägung als Erlaubnistatbestand für wissenschaftliche oder historische Forschungszwecke sowie zu statistischen Zwecken würde als „§ 27 Abs. 1 BDSG i. V. m. Art. 9 Abs. 4 DS-GVO“ dargestellt werden (müssen) – aufgrund des in Art. 9 Abs. 1 DS-GVO enthaltenen Verbots der Verarbeitung von besonderen Kategorien personenbezogener Daten muss immer auch ein Erlaubnistatbestand aus Art. 9 DS-GVO diese Verarbeitung (mit) erlauben. Entsprechend ist das EuGH-Urteil auch auf nationale Erlaubnistatbestände zur Verarbeitung von besonderen Kategorien personenbezogener Daten anzuwenden und es muss immer auch mindestens einer der in Art. 6 Abs. 1 DS-GVO angeführten Rechtfertigungsgründe erfüllt sein.

Die in § 27 Abs. 1 BDSG enthaltene Interessensabwägung findet natürlich in Art. 6 Abs. 1 lit. f DS-GVO ihre Entsprechung. Aber für jede nationale Regelung, die von einem Verantwortlichen angewendet wird, ist immer auch ein erfüllter Rechtfertigungsgrund aus Art. 6 Abs. 1 DS-GVO zu finden und anzugeben, wenn die Verarbeitung von in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien personenbezogener Daten legalisiert werden soll.

Im deutschen Recht existiert eine Vielzahl von entsprechenden Erlaubnistatbeständen, z. B. finden sich diverse Erlaubnistatbestände in §§ 64a ff. SGB X. Findet sich keine Entsprechung in den in Art. 6 Abs. 1 lit. a bis e DS-GVO genannten Rechtfertigungsgründen, ist in diesen Fällen eine Interessensabwägung nach Art. 6 Abs. 1 lit. f DS-GVO erforderlich. Entsprechend Rechtsprechung des EuGH sind bei einer Interessensabwägung immer drei Voraussetzungen zu erfüllen:[18]

1. Es muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden.
2. Die Verarbeitung der personenbezogenen Daten muss zur Verwirklichung des berechtigten Interesses erforderlich sein. Hierbei ist stets zu prüfen, „ob das berechtigte Interesse an der Verarbeitung der Daten nicht in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden kann, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch die Art. 7 und 8 der Charta garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen“.

[17] EuGH, Urt. v. 2023-03-30, Rechtssache C-34/21. Rn. 65, 71. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0034

[18] EuGH, Urt. v. 2023-12-07, Rechtssache C-26/22, C-64/22. Rn. 75 bis 80. Online, zitiert am 2023-12-29; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62022CJ0026

3. Die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, dürfen nicht überwiegen. Hinweise zum Umgang mit dieser Fragestellung finden sich weiter oben in Abschnitt zur Regelung in Art. 9 Abs. 2 lit. d DS-GVO.

Eine Verarbeitung darf bei Erfordernis einer Interessensabwägung trotz des Vorliegens eines nationalen Erlaubnistatbestandes daher nur durchgeführt werden, wenn die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person gegenüber den berechtigten Interessen des Verantwortlichen (oder eines Dritten) nicht überwiegen.

Fazit

Das Urteil des EuGH vom 21. Dezember 2023 in der Rechtssache C-667/21 besitzt zumindest in organisatorischer Hinsicht großen Einfluss bei jeglicher Verarbeitung von besonderen Kategorien personenbezogener Daten, denn Verantwortliche müssen neben einer in Art. 9 DS-GVO oder im nationalen Recht enthaltenen Rechtsgrundlage für die Verarbeitung von besonderen Kategorien personenbezogener Daten immer auch die Erfüllung von mindestens einem in Art. 6 Abs. 1 DS-GVO enthaltenen Rechtfertigungsgrund nachweisen können.

In den meisten Fällen werden Verantwortliche in Art. 6 Abs. 1 lit. a bis e DS-GVO zu Art. 9 Abs. 2 DS-GVO sowie zu nationalen Erlaubnistatbeständen korrespondierende Vorgaben finden.

In den wenigen Fällen, wo dies dem Verantwortlichen nicht möglich ist, muss eine Interessensabwägung gem. Art. 6 Abs. 1 lit. f DS-GVO durchgeführt werden und die Verarbeitung darf nur durchgeführt werden, wenn die (legitimen) Interessen des Verantwortlichen überwiegen und die Ziele der Verarbeitung nicht anders erreicht werden können.

Der EuGH äußerte sich in diversen Urteilen zur Interessensabwägung, sodass Verantwortliche daraus resultierende Vorgaben beachten müssen. Es kann dabei vorkommen, dass in wenigen Fällen, in denen eine Interessensabwägung überwiegende Interessen betroffener Personen ergibt, auf eine Verarbeitung auch verzichtet werden muss. [Absatz einfügen]

Weiterhin müssen Verantwortliche beachten, dass die Nutzung eines in Art. 6 Abs. 1 lit. f DS-GVO enthaltenen Rechtfertigungsgrundes einer Verarbeitung immer auch eine Informationspflicht nach Art. 13 Abs. 1 lit. d bzw. Art. 14 Abs. 2 lit. b DS-GVO bedingt.

Über den Autor

Dr. Bernd Schütze
beschäftigt sich seit 1995 mit den datenschutzrechtlichen Aspekten innerhalb der Gesundheitsversorgung. Nach gut dreißigjähriger beruflicher Tätigkeit in verschiedenen Krankenhäusern arbeitet Dr. Schütze seit 2014 als „Senior Experte Medical Data Security“ bei der Deutschen Telekom Healthcare and Security Solutions GmbH. Als Lehrbeauftragter ist er zudem an verschiedenen Hochschulen tätig und veröffentlicht regelmäßig Beiträge in Büchern und Fachzeitschriften. Dr. Schütze leitet die Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ der GMDS, gehört zum Leitungskreis der Arbeitsgruppe „Datenschutz & IT-Sicherheit“ des bvitg und ist Mitglied des Ausschusses „Recht & Politik“ des BvD.

Anzeige

Piltz Legal update
Seminare und Veranstaltungen von Piltz Legal

Seminar
DSGVO-Bußgelder und Schadenersatzansprüche von Betroffenen
Vermeidung und Verteidigung
25. April 2024 – in Frankfurt am Main

Christina Rost
Leitung Stabsstellen Öffentlichkeitsarbeit und Justiziariat/ Persönliche Referentin HBDI

Dr. Carlo Piltz
Rechtsanwalt, Partner bei Piltz Legal

Adina Apartment Hotel Frankfurt Neue Oper
Start 9 Uhr, Ende ca. 14 Uhr
110,00 EUR (netto) pro Teilnehmer

Weitere Informationen

Piltz Rechtsanwälte PartGmbB | +49 30 814 53 50 00 | events@piltz.legal | www.piltz.legal

Auswirkungen der Gerichtsentscheidungen zu DSGVO-Bußgeldern

Welche Folgen haben die Entscheidungen für die Praxis?

Tim Wybitul, Jonas Kraus

A. Zusammenfassung

Der Europäische Gerichtshof (EuGH) hat in seiner Entscheidung vom 05.12.2023, C 807/21, wichtige Aussagen zur Verhängung von Bußgeldern wegen Datenschutzverstößen getroffen. Im Nachgang hierzu hat das Kammergericht Berlin (KG) das weitere Verfahren an das Landgericht Berlin zurückverwiesen (Az. 3 Ws 250/21). Bußgelder nach Art. 83 DSGVO sind aus wirtschaftlicher Sicht neben Schadensersatzforderungen typischerweise eines der größten Risiken für Unternehmen im Bereich des Datenschutzrechts. Die Entscheidungen sind für die datenschutzrechtliche Praxis der Unternehmen und ihrer Datenschutzbeauftragten daher von erheblicher praktischer Relevanz.

Eine verschuldensunabhängige Unternehmenshaftung, eine sogenannte "strict liability", hat der EuGH entgegen der Forderung der Datenschutzbehörden abgelehnt. Nach der Entscheidung steht fest, dass ein datenschutzrechtliches Bußgeld die Feststellung eines zurechenbaren vorsätzlichen oder fahrlässigen Handelns eines Mitarbeiters erfordert, welcher im Namen des Unternehmens handelt. Auch wenn die Datenschutzbehörden einen schuldhaften DSGVO-Verstoß nachweisen müssen, ist es nach der Entscheidung des EuGH hierfür nicht erforderlich, dass sie dabei einzelne handelnde Mitarbeiter identifizieren.

Zudem hat sich der EuGH zum einschlägigen Bußgeldrahmen geäußert: Für einen Datenschutzverstoß wird der maximale Bußgeldrahmen anhand des Umsatzes der „wirtschaftlichen Einheit“ berechnet. Für konzernangehörige Unternehmen bedeutet dies nach der Entscheidung des EuGH, dass hierfür der Jahresumsatz der wirtschaftlichen Einheit i. S. v. Artt. 101, 102 AEUV heranzuziehen ist, also vereinfacht gesprochen der des Konzerns. Dieser Punkt ist von erheblicher Bedeutung. Denn dies ist in den Artikeln der DSGVO selbst gar nicht geregelt. Nach der bisherigen Rechtsprechung des EuGH muss ein derart wesentlicher Aspekt in den Artikeln der DSGVO und nicht – wie hier in den Erwägungsgründen – geregelt sein. Dennoch steht nun fest, dass sich der maximale Bußgeldrahmen für ein konzernangehöriges Unternehmen in Zukunft wohl nach dem Umsatz des gesamten Konzerns richten wird.

Für die Praxis der Datenschutzbeauftragen in Unternehmen ergeben sich aus dem Urteil des EuGH insbesondere die folgenden Schlussfolgerungen:

- Positionen der Aufsichtsbehörden sind Rechtsauffassungen. Die Aufsichtsbehörden sind keine Gerichte und damit – genau wie Unternehmen – nur Rechtsanwender. Die Entscheidung des EuGH hat der Auffassung der Aufsichtsbehörden in Bezug auf eine „strict liability“ eine klare Absage erteilt. Die Entscheidung zeigt also, dass es für Unternehmen und ihre Datenschutzbeauftragte durchaus Sinn machen kann sich gegen überzogene Behördenanforderungen zur Wehr zu setzen.
- Der EuGH hat klargestellt, dass ein Bußgeld gegen ein Unternehmen (i) die Feststellung einer schuldhaft begangenen Tat sowie vor allem (ii) den konkreten Nachweis der schuldhaften Tat erfordert. Unternehmen und ihre Datenschutzbeauftragten sollten überlegen, in welchen Situationen sie den Datenschutzbehörden den von diesen gescheuten „Aufwand“ nicht abnehmen und den Behörden – im Rahmen des rechtlich Erlaubten – weniger Informationen proaktiv bereitstellen und Fragen der Behörden tendenziell zurückhal-

tend beantworten. Anderenfalls erleichtert dies es den Datenschutzbehörden den rechtsstaatlich gebotenen Nachweis zu führen, was die weitere Verteidigung deutlich erschweren und viel Geld kosten kann.

- Die Einhaltung datenschutzrechtlicher Vorschriften durch Unternehmen ist infolge der Entscheidung des EuGH noch wichtiger geworden, insbesondere im Konzernumfeld. Zum einen hat der EuGH das deutsche Bußgeldrecht insoweit bestätigt, dass die Behörde für eine Sanktionierung des Unternehmens keine konkret handelnden Mitarbeiter identifizieren muss. Zum anderen hat der EuGH klargestellt, dass im Konzernumfeld wegen Artt. 101, 102 AEUV für die Bestimmung des maximalen Bußgeldrahmens der Jahresumsatz des gesamten Konzerns als „wirtschaftliche Einheit" herangezogen wird. Den Datenschutzbehörden ist es insofern in Zukunft leichter möglich bei Verstößen vermeintlich „kleiner" Tochtergesellschaften empfindliche Bußgelder zu verhängen. Die beste Verteidigung hiergegen ist es bereits von Anfang an eine Verletzung der Vorgaben der DSGVO zu vermeiden.
- Sorgen machen hier allerdings einige Aussagen des KG aus dem Beschluss vom 22.01.2024. Danach solle „selbst eine normentsprechende Organisation […] – jedenfalls in aller Regel – nicht zur Exkulpation" führen, da „dies dem Effektivitätsgrundsatz des europäischen Rechts [entspricht]." Diese Aussagen sind schon in rechtlicher Hinsicht unzutreffend. Derartige Vorgaben hat der EuGH gerade nicht gemacht. Noch schlimmer wären aber die Praxisfolgen dieser Rechtsauffassung. Denn dann könnte selbst eine umfassend datenschutzkonforme („normentsprechende") Organisation nicht vor Bußgeldern schützen. Damit wären Rolle und Bedeutung der Datenschutzbeauftragten und des Datenschutzes in Unternehmen stark eingeschränkt. Es bleibt aber zu hoffen, dass andere deutsche Gerichte (und Behörden) dieser Fehlinterpretation des EuGH durch das KG nicht folgen werden.

B. Hintergrund der Entscheidung

In einem Bußgeldverfahren hatte die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) im Jahr 2019 ein Bußgeld unmittelbar gegen ein Unternehmen verhängt. Die BlnBDI hatte dieses dabei als „Betroffenen" im Sinne des OWiG, also als Täter des vermeintlichen Verstoßes gegen die DSGVO, angenommen. In ihrem Bußgeldbescheid hatte die Behörde keinen Nachweis für eine schuldhaft begangene Tat geführt. Das deutsche Bußgeldrecht nach dem OWiG setzt dies bei einer Sanktionierung eines Unternehmens aber zwingend voraus. Die BlnBDI ging davon aus, dass i. R. v. Art. 83 DSGVO eine „strict liability" gelte, so dass es entgegen dem Rechtsstaatsprinzip auf einen Tatnachweis nicht ankomme. Das betroffene Unternehmen ging gegen den Bußgeldbescheid vor, welchen das LG Berlin dann aufhob. Zudem stellte das Gericht das Verfahren nach § 206a StPO iVm §§ 46, 71 OWiG ein. Hiergegen legte die Berliner StA sofortige Beschwerde zum KG ein, welches die entscheidungserheblichen Fragen um die Auslegung von Art. 83 DSGVO im Rahmen eines Vorabentscheidungsverfahrens nach Art. 267 AEUV dem EuGH zur Auslegung vorlegte (Vorlagebeschl. v. 06.12.2021, 3 Ws 250/21).

Der EuGH ist bezüglich Tatsachenfragen und nationalen Rechtsfragen streng an die Darstellungen und Wertungen des KG gebunden. Hiervon konnte der EuGH auch bei den teilweise erkennbaren erheblichen Zweifeln nicht abweichen. Der EuGH war vielmehr ausschließlich zur verbindlichen Entscheidung der auslegungsbedürftigen, bislang ungeklärten Fragen des Unionsrechts berufen.

C. Position der Datenschutzbehörden

In der datenschutzrechtlichen Praxis orientieren sich Unternehmen zur Vermeidung von aufsichtsbehördlichen Maßnahmen meist an der Rechtsauffassung der Datenschutzbehörden. Dass dies für Unternehmen nicht immer zielführend ist, zeigt die Position der Datenschutzbehörden in Bezug auf eine „strict liability" geradezu exemplarisch.

Das gemeinsame Abstimmungsgremium der deutschen Datenschutzbehörden, die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), ging vor der Entscheidung des EuGH von einem „supranationalem Sanktionsregime" nach Maßgabe ihrer Interpretation des Art. 83 DSGVO aus (siehe beispielsweise DSK-Stellungnahme v. 05.01.2023; abrufbar unter https://www.datenschutzkonferenz-online.de/media/st/20230118_DSK_Stellungnahme_Datenschutzverstoesse_von_Unternehmen.pdf).

Dieses sollte den Behörden aus Sicht der DSK die Verhängung von Bußgeldern ohne unnötigen Aufwand und in effizienter Weise ermöglichen. Dabei formulierte die DSK klar, dass eine „strict liability" in erster Linie Tatfeststellungen und Tatnachweise verhindern sollte, um den Aufsichtsbehörden den hierfür nötigen „Aufwand" zu ersparen. Dabei überging die DSK, dass entsprechende Feststellungen beziehungsweise Nachweise nach dem deutschen Rechtsstaatsprinzip und nach § 66 OWiG geboten sind.

Die in der DSK repräsentierten Behörden sind nach Art. 20 Abs. 3 GG an Recht und Gesetz sowie an das Prinzip der Gesetzmäßigkeit der Verwaltung gebunden. Dennoch formulierte die DSK ausdrücklich, dass sie vor allem den „enormen Aufwand" bei der Ausermittlung von Verstößen in großen Unternehmen mit Konzernstrukturen vermeiden wollte: „Den Nachweis eines Organisations- oder Überwachungsverschuldens einer Leitungsperson erbringen zu kön-

nen, wird schwieriger, je größer das Unternehmen und seine organisatorischen Verflechtungen sind, insbesondere bei großen börsennotierten Konzernen“ (DSK-Stellungnahme v. 05.01.2023, S. 15). Insbesondere sei „der Nachweis […] regelmäßig mit einem erheblichen Aufwand verbunden“ (DSK-Stellungnahme vom 05.01.2023, S. 16).

D. EuGH: Keine „strict liability“

Der EuGH hat der geforderten „strict liability“ eine klare Absage erteilt. Ein auf Grundlage von Art. 83 DSGVO verhängtes Bußgeld erfordert nach Ansicht der Großen Kammer des EuGH zwingend den Nachweis, „dass der Verantwortliche, der eine juristische Person und zugleich ein Unternehmen ist, einen in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoß vorsätzlich oder fahrlässig begangenen hat“ (Urt. v. 05.12.2023 – C-807/21, Antwort auf Vorlagefrage 2). Dies bestätigt aus Sicht des EuGH neben dem klaren Wortlaut von Art. 83 Abs. 2 DSGVO auch die Systematik und der Zweck der DSGVO insgesamt.

Für die Praxis bedeutet dies, dass die Verhängung eines Bußgeldes gegen ein Unternehmen (i) die Feststellung einer schuldhaft begangenen Tat sowie (ii) den konkreten Nachweis der schuldhaften Tat erfordert.

E. Anforderungen des EuGH für die „Zurechnung“ eines DSGVO-Verstoßes

Aufgrund der vom KG gestellten Vorlagefragen befasste sich der EuGH in seiner Entscheidung vor allem mit den Anforderungen an die Identifizierung von Mitarbeitern, die im Namen des Unternehmens als datenschutzrechtlich Verantwortliche handeln. Letztlich ging es dabei um die Fragestellung, ob ein Bußgeld gegen ein Unternehmen voraussetzt, dass die Behörde zuvor eine (individualisierte) natürliche Person identifizieren muss, welche den Verstoß gegen die DSGVO begangen hat.

I. Sanktionierung von juristischen Personen im deutschen Recht

Das deutsche Recht setzt eine solche eindeutige Identifizierung natürlicher Personen nicht voraus. Vielmehr ist es aufgrund von § 30 Abs. 4 OWiG im Wege einer sogenannten selbstständigen Verbandsbuße möglich dem Unternehmen die Verletzung der Aufsichtspflicht durch die Unternehmensleitung zuzurechnen, wenn diese einen Gesetzesverstoß von Mitarbeitern nicht entsprechend ihrer gesetzlichen Verpflichtungen verhindert (vgl. §§ 30, 130, 9 OWiG). Es ist hierfür nicht erforderlich, dass eine Behörde einen konkret handelnden Mitarbeiter unterhalb der Leitungsebene oder konkret verantwortliche Angehörige der Unternehmensleitung benennt.

II. Vorgaben des KG, an welche der EuGH gebunden war

Der Vorlagebeschluss des KG erwähnte die für die Sanktionierung von juristischen Personen im deutschen Recht zentrale Vorschrift des § 130 OWiG nicht einmal. Das KG stellte in seinem Vorlagebeschluss also eine unrichtige Rechtslage dar, was auch zu einem deutlichen Widerspruch der Vertreter der Bundesrepublik Deutschland in der Verhandlung vor dem EuGH führte.

Aufgrund der Verfahrensgrundsätze des Vorabentscheidungsverfahrens nach Art. 267 AEUV war der EuGH für seine Entscheidung dennoch an die Vorgaben des KG gebunden, was der EuGH selbst folgendermaßen beschrieb: „Es ist darauf hinzuweisen, dass der Gerichtshof in Bezug auf die Auslegung von Bestimmungen des nationalen Rechts grundsätzlich gehalten ist, die sich aus der Vorlageentscheidung ergebenden rechtlichen Würdigungen zugrunde zu legen. Nach ständiger Rechtsprechung ist der Gerichtshof nämlich nicht befugt, das innerstaatliche Recht eines Mitgliedstaats auszulegen“ (Urt. v. 05.12.2023 – C-807/21, Rn. 36).

III. Vom EuGH aufgestellte Vorgaben

Vor diesem Hintergrund stellte der EuGH klar, dass die von ihm in der Entscheidung aufgestellten Vorgaben zur Zurechnung eines DSGVO-Verstoßes nur für Fälle gelten sollen, in denen es unter dem anwendbaren nationalen Recht notwendig ist, eine konkrete, den Vorgaben der DSGVO zuwider handelnde Person zu identifizieren (Urt. v. 05.12.2023 – C-807/21, Rn. 37).

Konkret sollen Unternehmen laut EuGH für Verstöße haften, die von Leitungspersonal begangen wurden, aber auch für Verstöße, welche sonstige Personen begangen haben, „die im Rahmen der unternehmerischen Tätigkeit und im Namen dieser juristischen Person handel[n]“ (Urt. v. 05.12.2023 – C-807/21, Rn. 44). Außerdem „muss es möglich sein, die in Art. 83 DSGVO für solche Verstöße vorgesehenen Geldbußen unmittelbar gegen juristische Personen zu verhängen, wenn diese als für die betreffende Verarbeitung Verantwortliche eingestuft werden können“ (Urt. v. 05.12.2023 – C-807/21, Rn. 44).

Tatsächlich sieht das deutsche Recht dies bereits vor. Eine Zurechnung von Aufsichtspflichtverletzungen der Unternehmensleitung und damit eine Haftung für Bußgelder ist über §§ 30, 130, 9 OWiG möglich. Außerdem ist nach § 30 OWiG eine unmittelbare Sanktionierung von Unternehmen möglich – das Unternehmen ist dabei eine sogenannte Nebenbeteiligte. Über § 30 Abs. 4 OWiG ist dabei auch dann die Möglichkeit einer unmittelbaren, selbstständigen Sanktionierung

des Unternehmens gegeben, wenn kein Verfahren gegen die in § 30 Abs. 1 Nr. 1 bis Nr. 5 OWiG genannten Leitungspersonen eingeleitet oder ein solches eingestellt wird.

Einer umfassenden Analogie zum unionsrechtlichen Wettbewerbsrecht sowie einem supranationalen Sanktionsregime erteilt der EuGH damit eine klare Absage. Nach dem EuGH sind Art. 58 Abs. 2 DSGVO und Art. 83 Abs. 1 bis Abs. 6 DSGVO „dahin auszulegen, dass sie einer nationalen Regelung entgegenstehen, wonach eine Geldbuße wegen eines in Art. 83 Abs. 4 bis 6 DSGVO genannten Verstoßes gegen eine juristische Person in ihrer Eigenschaft als Verantwortliche nur dann verhängt werden kann, wenn dieser Verstoß zuvor einer identifizierten natürlichen Person zugerechnet wurde" (Urt. v. 05.12.2023 – C-807/21, Antwort auf Vorlagefrage 1).

Im deutschen Recht ist dies aber gerade nicht der Fall. Wie bereits dargestellt, ist es auch nach dem OWiG nicht notwendig individuelle Mitarbeiter, die durch ihre Handlungen gegen die Vorgaben der DSGVO verstoßen, oder konkretes Leitungspersonal, das seine Aufsichtspflichten verletzt hat, zu identifizieren. Bei einer verständigen Würdigung der Aussagen des EuGH bleibt also kein Raum für Zweifel an der Anwendbarkeit des nationalen Bußgeldrechts.

F. Festlegung des maximalen Bußgeldrahmens laut EuGH

Für die datenschutzrechtliche Praxis und die Datenschutzbeauftragten von Unternehmen sind darüber hinaus die vom EuGH zur Bestimmung des einschlägigen Bußgeldrahmens getroffenen Vorgaben von erheblicher Bedeutung. Dies gilt insbesondere, da aus kommerzieller Sicht die Verhängung eines Bußgeldes neben Schadenersatzforderungen nicht selten das größte Risiko im Zusammenhang mit Verstößen gegen die DSGVO darstellt. Obwohl die Vorlagefragen des KG die Thematik überhaupt nicht betrafen, sah sich der EuGH im Rahmen eines Obiter Dictum dazu veranlasst zur Festlegung des Bußgeldrahmens nach Art. 83 Abs. 4 bis Abs. 6 DSGVO Stellung zu nehmen.

Dabei stellte der EuGH in Bezug auf konzernangehörige Unternehmen klar, dass für die Bestimmung des für Art. 83 Abs. 4 beziehungsweise Abs. 5 DSGVO einschlägigen Jahresumsatzes die wirtschaftliche Einheit nach Art. 101, 102 AEUV heranzuziehen ist (Urt. v. 05.12.2023 – C-807/21, Rn. 55 bis 59). Aufgrund der Bezugnahme von ErwG 150 S. 3 DSGVO auf die Regelungen des unionsrechtlichen Kartellrechts ist für den EuGH die relevante „wirtschaftliche Einheit" der gesamte Konzern – nicht das bloße, konkret gegen die DSGVO verstoßende konzernangehörige Unternehmen.

G. Praktische Konsequenzen für die datenschutzrechtliche Praxis im Unternehmen

Unternehmen und ihre Datenschutzbeauftragten können aus der Entscheidung des EuGH einige Schlüsse für die Verteidigung gegen mögliche Bußgelder ziehen. Diese können den Unternehmen helfen das Risiko von rechtskräftig gegen die juristische Person verhängte Bußgelder zu reduzieren. Beispielsweise sollte man die neuere Rechtsprechung zum Anlass nehmen die Offenlegung von möglichen Schwachstellen gegenüber Datenschutzbehörden zu überdenken. Nachdem Gerichte und Behörden hier zunehmend strenge Maßstäbe anlegen, sollten Unternehmen in laufenden Verfahren gründlich prüfen, ob sie von Aussageverweigerungsrechten Gebrauch machen.

H. Ausblick

Zwischenzeitlich hat das KG den Rechtsstreit nach der Entscheidung des EuGH an das LG Berlin zurückverwiesen. Es bleibt zu hoffen, dass sich andere deutsche Gerichte nicht der Auffassung des KG anschließen, dass selbst eine vollständig DSGVO-konforme Organisation nicht vor Bußgeldern schützen solle. Den Vorgaben des EuGH entspricht diese Folgerung jedenfalls nicht.

Es ist zudem davon auszugehen, dass sich das Verfahren noch über einige Zeit hinziehen wird, denn bislang betraf es ausschließlich prozessuale Fragen. Die materiellrechtlichen Fragen des Verfahrens, etwa wann personenbezogene Daten gelöscht werden müssen oder wie sie archiviert werden können, sind bislang kein Gegenstand richterlicher Kontrolle gewesen. Es liegt nahe, dass sich der EuGH vor allem mit den entscheidungsrelevanten Fragen zur Löschung von Daten, aber auch mit den hier angesprochenen Fragen noch einmal auseinandersetzen wird.

Über die Autoren

Tim Wybitul
ist Partner bei Latham & Watkins und ein führender Datenschutzanwalt. Er berät deutsche und globale Unternehmen in komplexen Fragen des Datenschutzes und der Cybersecurity. Er vertritt Mandanten in Datenschutzstreitigkeiten vor Gerichten, in behördlichen Verfahren und in anderen datenschutzrechtlichen Auseinandersetzungen.

Jonas Kraus
ist Rechtsanwalt und Associate bei Latham & Watkins. Seine Beratungspraxis umfasst die rechtliche Beratung internationaler sowie nationaler Unternehmen mit einem Schwerpunkt auf das europäische und deutsche Datenschutzrecht sowie damit verbundener Rechtsgebiete. Er berät und vertritt Unternehmen regelmäßig im Zusammenhang mit gerichtlichen und behördlichen Verfahren.

ANONYMISIERUNG UND PSEUDONYMISIERUNG AUS DATENSCHUTZRECHTLICHER SICHT

Andrea Backer-Heuveldop, Regina Mühlich, Dr. Bernd Schütze

Seitens der Datenwirtschaft besteht eine immer größere Nachfrage nach personenbezogenen Daten. Durch das verstärkte Aufkommen des Themas „Künstliche Intelligenz" (KI) ist die Nachfrage nach personenbezogenen Daten weiter gestiegen. Häufig wird versucht die Bürger durch Anonymisierung oder Pseudonymisierung davon zu überzeugen, dass ihre Daten durch diese Maßnahmen nicht missbraucht werden können und Daten daher zur Verfügung gestellt werden sollten. Richtig ist, dass sowohl die Pseudonymisierung als auch die Anonymisierung dazu dienen können die Risiken für die Betroffenen bei der Verarbeitung ihrer Daten zu verringern, aber auch durch diese Maßnahmen können Risiken nicht ausgeschlossen werden.

Insbesondere in Deutschland wird von verschiedenen Akteuren eine Definition des Begriffs „Anonymisierung" gefordert; dass es eine europarechtliche Definition gibt scheint denjenigen, die sich von der Forderung einen effektiven Schutz vor Missbrauch bei der Verarbeitung personenbezogener Daten versprechen, unbekannt zu sein.

Offensichtlich gibt es verschiedene Fragen im Zusammenhang mit Anonymisierung und Pseudonymisierung. Eine Gruppe von Mitgliedern verschiedener Verbände hat sich zusammengefunden, um eine Praxishilfe[1] für den Umgang mit diesen Fragen insbesondere im Gesundheitswesen zu erstellen. In diesem Beitrag werden einige wichtige Punkte angesprochen, für eine ausführlichere Darstellung wird auf die Praxishilfe selbst verwiesen, in der neben der rechtlichen Betrachtung auch Hinweise zur Durchführung einer Anonymisierung bzw. Pseudonymisierung zu finden sind.

Anonymisierung und Pseudonymisierung: Begriffsbestimmung

Der Begriff der Pseudonymisierung ist in Art. 4 Ziff. 5 DS-GVO definiert, diese Definition ist allgemein bekannt. Daher wird an dieser Stelle auf eine weitere Erläuterung verzichtet.

Anonymisierung wird in Art. 3 Ziff. 7 der Richtlinie (EU) 2019/1024[2] wie folgt definiert:

> *„Anonymisierung" den Prozess, in dessen Verlauf Dokumente in anonyme Dokumente umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten so anonym gemacht werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.*

[1] GMDS, BvD, bvitg: Arbeitshilfe zur Anonymisierung/Pseudonymisierung. Stand 2024-01. Online, zitiert am 2024-02-04; verfügbar unter https://www.bvdnet.de/wp-content/uploads/2024/02/praxishilfe_anonymisierung_pseudonymisierung.pdf https://gesundheitsdatenschutz.org/html/pseudonymisierung_anonymisierung.php

[2] Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors. Online, zitiert am 2023-12-30; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019L1024&rqid= 1697259421370

Bei der Auslegung dieser Begriffsbestimmung ist zu beachten, dass sich Art. 3 Ziff. 7 der Richtlinie (EU) 2019/1024 mit dem Begriff „Dokumente“ befasst, der seinerseits in Art. 3 Ziff. 6 der Richtlinie (EU) 2019/1024 definiert ist:

> *„Dokument“*
>
> *a) jeden Inhalt unabhängig von der Form des Datenträgers (auf Papier oder in elektronischer Form oder als Ton-, Bild- oder audiovisuelles Aufnahme); oder*
>
> *b) einen beliebigen Teil eines solchen Inhalts.*

Der Begriff „Dokument“ ist also wesentlich weiter gefasst, als dies im deutschen Sprachgebrauch üblich ist. Diese Definition entspricht der Definition der internationalen Norm ISO/IEC 29100[3].

Europäische Richtlinien müssen durch nationale Rechtsakte umgesetzt werden.[4] Im Falle der Begriffsdefinition der Anonymisierung ist dies durch § 3 Ziff. 12 Datennutzungsgesetz geschehen:

> *„Anonymisierung“ ist der Prozess, in dessen Verlauf personenbezogene Daten in Daten umgewandelt werden, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder derart in Daten umgewandelt werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.*

Unter Berücksichtigung der Bedeutung des Wortes „Dokument“ in der europäischen Regelung kommt die deutsche Umsetzung mit der Verwendung des Wortes „Daten“ dem Sinngehalt der Regelung sehr nahe. Gleichwohl empfiehlt es sich in Zweifelsfällen zumindest parallel die Begriffsbestimmung in Art. 3 Ziff. 7 der Richtlinie (EU) 2019/1024 heranzuziehen, da – wie der BGH entschieden hat[5] – der Gesetzgeber die europäischen Vorgaben zu beachten hat, sodass gegebenenfalls auch eine europarechtskonforme Auslegung der nationalen Normen zu erfolgen hat.

Somit gibt es sowohl für die Pseudonymisierung als auch für die Anonymisierung Legaldefinitionen.

Braucht es einen Erlaubnistatbestand für die Anonymisierung oder Pseudonymisierung?

In Art. 4 Ziff. 2 DS-GVO findet sich die Begriffsbestimmung von „Verarbeitung“, die leichter zu betrachten ist, wenn man von der beispielhaften Aufzählung der Verarbeitungsvorgänge absieht:

> *„Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten [...]*

Jeder Vorgang im Zusammenhang mit personenbezogenen Daten stellt somit eine Verarbeitung dar, insbesondere also auch die Anonymisierung oder Pseudonymisierung. Gemäß Art. 5 Abs. 1 lit. a DS-GVO müssen personenbezogene Daten insbesondere auch auf „rechtmäßige Weise“ verarbeitet werden. Nach Art. 6 Abs. 1 DS-GVO ist eine Verarbeitung nur dann rechtmäßig, wenn mindestens eine der in Art. 6 Abs. 1 lit. a-f DS-GVO genannten Bedingungen

[3] ISO/IEC 29100:2011: „Information technology - Security techniques - Privacy framework. Online, zitiert am 2023-12-30; verfügbar unter https://www.iso.org/standard/45123.html bzw. Download pdf-Datei kostenlos unter https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Deutsche Übersetzung der Norm von 2011 wurde 2020 vom Beuth-Verlag veröffentlicht: https://www.beuth.de/de/norm/din-en-iso-iec-29100/325198919

[4] Deutscher Bundestag, Wissenschaftliche Dienste: Kurzinformation – Umsetzung von EU-Richtlinien und Verfassungsrecht. Online, zitiert am 2023-12-30; verfügbar unter https://www.bundestag.de/resource/blob/899872/33b2422d86eab34c741b67207ab1bda3/WD-3-045-22-pdf-data.pdf

[5] Siehe

- EuGH, Urt. v. 2019-10-01, Az. C-673/17. Online, zitiert am 2023-10-14; verfügbar unter https://dejure.org/2019,31907 bzw. Volltext Urteil beim EuGH unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1
- Darauf aufbauend: BGH, Urt. v. 2020-05-28, Az. I ZR 7/16. Siehe insbesondere Abschnitt „b“ des Urteilsspruches. Online, zitiert am 2023-10-14; verfügbar unter https://dejure.org/2020,12443 bzw. Volltext unter https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=107623&pos=0&anz=1

PRIVACYSOFT
Datenschutzmanagement as a Service

Datenschutz systematisch planen, organisieren, steuern und kontrollieren mit PRIVACYSOFT.

Vorlagen
Datenschutzdokumentation
Checklisten
E-Learning
Auditmodul
Mehrsprachig

Projekt 29 GmbH & Co. KG | Ostengasse 14
93047 Regensburg | www.privacysoft.de

erfüllt ist; bei der Verarbeitung der in Art. 9 Abs. 1 DS-GVO genannten besonderen Kategorien personenbezogener Daten muss zusätzlich[6] mindestens eine der in Art. 9 Abs. 2 DS-GVO genannten Ausnahmen vorliegen.

Sowohl die Pseudonymisierung als auch die Anonymisierung erfordern daher immer einen Erlaubnistatbestand, der diese Verarbeitung legalisiert.

Müssen betroffene Personen über eine Anonymisierung oder Pseudonymisierung informiert werden?

Eine Anonymisierung oder Pseudonymisierung stellt in der Regel eine Zweckänderung gegenüber dem Zweck dar, zu dem die Daten erhoben wurden. Häufig werden Daten auch anonymisiert oder pseudonymisiert, um die so verarbeiteten Daten anschließend zu einem anderen Zweck als dem ursprünglichen Zweck zu verarbeiten, wobei allerdings schon die Anonymisierung oder Pseudonymisierung selbst eine Verarbeitung zu einem anderen Zweck als den ursprünglichen darstellen, was beachtet werden muss.

Teilweise wird argumentiert, dass keine Zweckänderung vorliegt, wenn der neue Zweck „kompatibel" im Sinne des Art. 5 Abs. 1 lit. b DS-GVO ist. Dies ist falsch. Auch in diesen Fällen handelt es sich um einen anderen Zweck als den ursprünglichen Zweck, wie er auch in Art. 5 Abs. 1 lit. b DS-GVO ist: Der alte und der neue Zweck mögen zwar nicht miteinander unvereinbar sein, es handelt sich aber dennoch um verschiedene Zwecke.

Gemäß Art. 13 Abs. 4 bzw. Art. 14 Abs. 4 DS-GVO hat der Verantwortliche vor einer Verarbeitung zu einem anderen Zweck (also insbesondere auch noch vor der Pseudonymisierung/Anonymisierung) der/den betroffenen Person/en Informationen über diesen andren Zweck und alle weiteren relevanten Informationen gemäß Art. 13 und/oder Art. 14 Abs. 2 DS-GVO zur Verfügung zu stellen.

Eine Information der betroffenen Personen ist daher faktisch immer zwingend erforderlich und muss ggf. nachträglich, aber auf jeden Fall vor Beginn der Anonymisierung oder Pseudonymisierung, zu den bereits erteilten Informationen vorgenommen werden.

Ist die Pseudonymisierung oder Anonymisierung dagegen von Anfang an als Teil der Verarbeitung geplant, muss sie somit bei der Erfüllung der Informationspflichten im Rahmen der Erstinformation bei der Erhebung der Daten bereits berücksichtigt werden.

Umgang mit Nachweispflichten

Immer dann, wenn personenbezogene Daten verarbeitet werden, treffen den Verantwortlichen diverse Nachweispflichten, die sich aus verschiedenen Vorschriften der DS-GVO ergeben. Der EuGH legt diese in Art. 5 Abs. 2 DS-GVO verankerte Pflicht zum Nachweis der DS-GVO-konformen Verarbeitung sehr weit aus, auch im Sinne einer Beweislastumkehr.[7,8]

Da dies für jegliche Verarbeitung gilt, gelten die Nachweispflichten somit auch für eine Anonymisierung oder Pseudonymisierung. Nach ErwGr. 26 DS-GVO sollen die Vorgaben der DS-GVO zwar nicht für anonyme Daten gelten, jedoch muss der Verantwortliche, u. a. aufgrund der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO, zu jedem Zeitpunkt der Verarbeitung (und damit insbesondere auch während der gesamten Speicherdauer) nachweisen können, dass es sich bei den anonymisierten Daten zu jedem Zeitpunkt der Verarbeitung um anonyme Daten handelt. Der Nachweis der Anonymisierung stellt somit keinen einmaligen Vorgang dar, sondern ist als Prozess zu verstehen, der den gesamten Lebenszyklus der Daten begleitet.[9,10]

Gerade im Hinblick auf die sich sehr schnell entwickelnden technischen Möglichkeiten muss dieser Nachweis mit entsprechender Sorgfalt geführt werden und die dabei ange-

[6] EuGH, Urt. v-2023-07-04, Az. C-252/21, Rn. 73 bis 79. Online, zitiert am 2023-12-30; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0252

[7] Siehe z. B. EuGH, Urt. v. 2022-02-24, Az. C-175/20, Rn. 81 i. V. m. Rn. 77. Online, zitiert am 2023-12-30; verfügbar unter https://dejure.org/2022,3279 bzw. Volltext unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=254583&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

[8] EuGH, Urt. v. 2023-12-21, Az. C-667/21. Rn. 103. Online, zitiert am 2023-12-30; verfügbar unter https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:62021CJ0667

[9] EDSA (2021-02-02) EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research. Rn. 47. Online, zitiert am 2023-12-30; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/other-guidance/edpb-document-response-request-european-commission_en

[10] Siehe z. B. Gerichtsurteile:

- EuGH Urt. v. 2022-02-24, Az. C-175/20, Rn. 81 i. V. m. Rn. 77. Online, zitiert am 2023-12-30; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62020CJ0175
- BVerwG Urt. v. 2022-03-02, Az. 6 C 7.20, Rn. 49-51. Online, zitiert am 2023-12-30; verfügbar unter https://www.bverwg.de/020322U6C7.20.0
- OLG Stuttgart Urt. v. 2023-11-22, AZ. 4 U 20/23, Rn. 395-400. Online, zitiert am 2023-12-30; verfügbar unter https://www.landesrecht-bw.de/bsbw/document/JURE235012226

wandte Methodik muss mindestens dem Stand der Technik entsprechen.

So ist beispielsweise bei der Beurteilung, ob Daten als anonymisiert oder pseudonymisiert anzusehen sind, auch zu berücksichtigen, dass neue Daten zu einem bestehenden Datensatz hinzugefügt werden können, wodurch sich wiederum auch neue Möglichkeiten der Re-Identifizierung ergeben können.

Die Nachweispflicht aus Art. 5 Abs. 2 DS-GVO erfordert, dass der Nachweis erbracht wird, dass eine erfolgte Anonymisierung auch bei sich ändernden technischen Möglichkeiten oder neu gewonnenem Zusatzwissen irreversibel ist. Eine regelmäßige Überprüfung des Fortbestehens des Status „anonym" bzw. „pseudonym" und des damit verbundenen Schutzniveaus für die personenbezogenen Daten ist daher aus verschiedenen Gründen zwingend erforderlich und der entsprechende Prozess ist – ggf. einschließlich evtl. erforderlicher Kriterien, wann eine Überprüfung spätestens zu erfolgen hat – ebenso zu dokumentieren wie die Überprüfungen und deren Ergebnisse nachvollziehbar zu dokumentieren sind.

Muss ich anonyme Daten, die ich erhalte, auf Anonymität prüfen?

Wenn man Daten erhält, die grundsätzlich einer Person zugeordnet werden können, wird der Empfänger datenschutzrechtlich Verantwortlicher, wenn die Daten nicht als anonym, sondern als personenbezogen oder personenbeziehbar anzusehen sind.

Die (juristische oder natürliche) Person, von der man die Daten erhalten hat, kann bestenfalls grob abschätzen, welche technischen Möglichkeiten, Zusatzwissen usw. beim Empfänger vorhanden sind, sodass die Einstufung als „anonym" durch den Datenlieferanten falsch sein kann und man als Empfänger der Daten eine Prüfung vornehmen muss.

Ist man rechtlich Verantwortlicher, weil die erhaltenen Daten als personenbezogen oder personenbeziehbar anzusehen sind, unterliegt man allen Verpflichtungen des Datenschutzrechts.[11] Es ist nicht möglich, sich diesen Pflichten mit der Begründung zu entziehen „man habe dem Übermittler der Daten hinsichtlich der Anonymität der Daten vertraut". Die ständige Rechtsprechung des EuGH ist in dieser Hinsicht eindeutig: Der für die Verarbeitung Verantwortliche ist „verantwortlich".

Ursprünglich als anonym eingestufte Daten erweisen sich als personenbeziehbar

Im Laufe der Zeit kann es aufgrund technischer Entwicklungen, neu entdeckter mathematischer Verfahren usw. vorkommen, dass als anonym klassifizierte Daten nicht mehr als „anonym" eingestuft werden können, sondern als pseudonymisiert betrachtet werden müssen.

In diesem Fall sind alle Anforderungen der Datenschutzgesetze anzuwenden, wie beispielsweise:

- Darlegung der Rechtsgrundlage für die Verarbeitung;
- Gewährleistung der Betroffenenrechte wie z. B. Information der betroffenen Personen oder Löschung unrechtmäßig verarbeiteter Daten sowie Information der Empfänger der Daten hinsichtlich Erforderlichkeit der Löschung;
- Durchführung einer Datenschutz-Folgenabschätzung;
- Gewährleistung der Sicherheit der Verarbeitung

Daten wurden „anonym" übermittelt, nun erfolgt eine Re-Identifizierung

Der EuGH[12] hat in Leitsatz 3 entschieden, dass der Verantwortliche die Beweislast dafür trägt, dass die getroffenen Schutz-

[11] EuGH Urt. v. 2020-07-09, Az. C-272/19, Leitsatz: Art. 4 Nr. 7 DS-GVO ist dahin auszulegen, dass wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet, als „Verantwortlicher" im Sinne dieser Bestimmung einzustufen ist. Online, zitiert am 2023-12-30; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62019CJ0272&qid=1702720547526

[12] EuGH Urt. v. 2023-12-14, Az. C-340/21. Online, zitiert am 2023-12-30; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A62021CJ0340

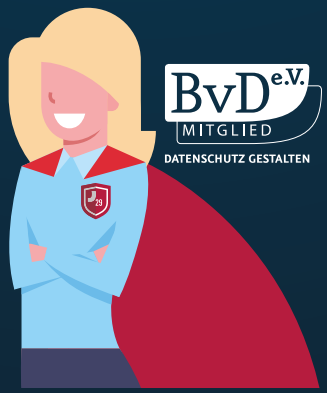
PRIVACYSOFT
Datenschutzmanagement as a Service

Lernen Sie PRIVACYSOFT im Rahmen einer kostenlosen Online-Demo kennen!

Unsere Experten zeigen Ihnen in aller Ruhe alle Funktionen und wie Sie ganz persönlich Ihr Datenschutzmanagement vereinfachen und effektivieren.

Bitte hinterlassen Sie uns Ihren Terminwunsch im Kontaktformular unter **www.privacysoft.de**

Oder rufen Sie einfach kurz bei uns an: **0941-29 86 93-0**



EXKLUSIV FÜR BvD-MITGLIEDER
DATENSCHUTZ-AWARENESS-ONEPAGER
Fordern Sie einfach und kostenlos unter www.privacysoft.de an.
Code: ONEPAGERBVD2023

Projekt 29 GmbH & Co. KG | Ostengasse 14
93047 Regensburg | www.privacysoft.de

maßnahmen angemessen waren. Dies bedeutet, dass der Verantwortliche, der anonymisierte Daten weitergegeben hat, die im Nachhinein re-identifiziert werden konnten, die Beweislast dafür trägt, dass die vorgenommene Anonymisierung zu Daten geführt hat, die den Anforderungen des Art. 3 Ziff. 7 der Richtlinie (EU) 2019/1024 entsprechen.

Im Falle einer gerichtlichen Überprüfung der getroffenen Maßnahmen hat ein Gericht nach dem genannten Urteil des EuGH (Rn. 45) eine materielle Prüfung der Maßnahmen anhand aller in Art. 32 genannten Kriterien sowie der Umstände des Einzelfalls und der dem Gericht insoweit zur Verfügung stehenden Beweismittel vorzunehmen, wobei die mit der betreffenden Verarbeitung verbundenen Risiken zu berücksichtigen sind und zu beurteilen ist, ob Art, Inhalt und Umsetzung dieser Maßnahmen diesen Risiken angemessen sind (Rn. 47).

Darüber hinaus kann der Verantwortliche im Fall einer unbefugten Offenlegung personenbezogener Daten durch Dritte, wie sie eine unbefugte Re-Identifizierung i. d. R. darstellen wird, gegenüber den Personen, die einen Schaden erlitten haben, schadensersatzpflichtig sein (vgl. das zitierte Urteil, Rn. 86), es sei denn, der Verantwortliche weist nach, dass er in keiner Weise für den Schaden verantwortlich ist.

Anonymisierung und „Big Data“

Die Methoden zum Schutz der Privatsphäre im Zusammenhang mit Big-Data-Anwendungen befinden sich noch in einem frühen Entwicklungsstadium, und diese Methoden können die Privatsphäre der betroffenen Personen aufgrund von Funktions- und Effizienzproblemen nicht gewährleisten.[13] Dies gilt insbesondere dann zu, wenn nicht vorhersehbar ist, welche Daten von wem zusammengeführt werden: In diesen Fällen wird durch die Zusammenführung immer kaum abschätzbares bzw. bewertbares Zusatzwissen zum eigentlich betrachteten Datensatz gewonnen, sodass eigentlich nur die Möglichkeit bleibt rechtlich, d. h. vertraglich, sicherzustellen, dass eine Zusammenführung des als „anonym“ betrachteten Datensatzes mit anderen, unbekannten Datensätzen verboten wird.

Pramanik et al. haben 2021[13] verschiedene Methoden zum Schutz der Privatsphäre im Zusammenhang mit Big Data-Anwendungen bewertet und versucht deren Vor- und Nachteile darzustellen. In diesem Review identifizierten die Autoren u. a. die Hauptschwächen der bestehenden Ansätze zum Schutz der Privatsphäre bei Big-Data-Analysen, gaben aber auch Empfehlungen für die Wirtschaftsakteure ab. Auch wenn sich keine der untersuchten Methoden direkt auf Anonymisierung oder Pseudonymisierung bezieht, bietet die Arbeit einen guten Überblick über die derzeit im Big-Data-Umfeld verwendeten Methoden.

Dr. Bernd Schütze

Da das Thema sicherlich auch in den nächsten Jahren nicht an Wichtigkeit verlieren wird, freut sich Dr. Schütze über Rückmeldungen zur Praxishilfe, insbesondere über Feedback aus dem Umfeld der medizinischen Forschung.

▶ schuetze@medizin-informatik.org

[13] Pramanik et al. (2021) Privacy preserving big data analytics: A critical analysis of state-of-the-Art. WIREs: e1387-e1392. https://doi.org/10.1002/widm.1387

FAZIT

Sowohl die Pseudonymisierung als auch die Anonymisierung sind wichtige Verfahren, um die Risiken für die betroffenen Personen bei der Verarbeitung ihrer Daten zu verringern, und sollten daher, wo immer es sinnvoll möglich ist, eingesetzt werden. Allerdings bedarf es einer intensiven Auseinandersetzung mit der Materie.

Eine Herausforderung für die zur Anonymisierung und Pseudonymisierung beratenden Datenschutzbeauftragten besteht darin sich selbst in die Methoden der Anonymisierung bzw. Pseudonymisierung einzuarbeiten und so einerseits Beschäftigte des Verantwortlichen bei diesen Themen beraten zu können, andererseits aber auch eine Bewertung der ergriffenen Maßnahmen durchführen zu können. So ermöglichen Datenschutzbeauftragte eine konsequente, wirksame und zuverlässige Anonymisierung und Pseudonymisierung und werden von Beschäftigten des Verantwortlichen als wertvolle Partner und Unterstützer wahrgenommen. Gerade im Zusammenhang mit der Anonymisierung werden immer wieder Thesen vertreten, die bei Betrachtung der rechtlichen Grundlagen kaum haltbar sind. Es wäre wünschenswert, wenn sich die Politik vor Gesetzesanpassungen fachlichen und sachkundigen Rat einholen würde. Insbesondere, wenn es um die Verarbeitung besonders sensibler Daten wie beispielsweise genetische oder Gesundheitsdaten geht: Personenbezogene oder personenbeziehbare Daten, die als vermeintlich „anonyme Daten" „der Welt" zur Verarbeitung zur Verfügung gestellt werden, sind letztlich nicht mehr einzufangen. Wirtschaft und Politik sind daher gut beraten sich vor Entscheidungen mit der Materie zu befassen. Die hier vorgestellte Praxishilfe will dazu einen Beitrag leisten.

Über die Autoren

Dr. Bernd Schütze
beschäftigt sich seit 1995 mit den datenschutzrechtlichen Aspekten innerhalb der Gesundheitsversorgung. Nach gut dreißigjähriger beruflicher Tätigkeit in verschiedenen Krankenhäusern arbeitet Dr. Schütze seit 2014 als „Senior Exporte Medical Data Security" bei der Deutschen Telekom Healthcare and Security Solutions GmbH. Als Lehrbeauftragter ist er zudem an verschiedenen Hochschulen tätig und veröffentlicht regelmäßig Beiträge in Büchern und Fachzeitschriften. Dr. Schütze leitet die Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen" der GMDS, gehört zum Leitungskreis der Arbeitsgruppe „Datenschutz & IT-Sicherheit" des bvitg und ist Mitglied des Ausschusses „Recht & Politik" des BvD.

Regina Mühlich
ist Wirtschaftsjuristin und Geschäftsführerin der AdOrga Solutions GmbH. Sie ist Datenschutzbeauftragte, CIPM, CIPP/U.S., Sachverständige für EDV und Datenschutz sowie Datenschutz-Auditorin und Compliance Officer und berät nationale und internationale Organisationen aus unterschiedlichsten Bereichen. Sie ist Dozentin an der EU Business School Munich sowie Advisory Board Member of health-h. Regina Mühlich ist Vorständin des BvD e.V. sowie Mitglied im Ausschuss Recht & Politik sowie Leiterin des Committee Law & Politics des EFDPO.

Andrea Backer-Heuveldop
ist fachlich geprüfte fachkundige Datenschutzbeauftragte nach dem Ulmer Modell. Sie ist als externe Datenschutzbeauftragte bei ds-quadrat Unternehmensberatung GmbH & Co. KG im Gesundheitswesen tätig und engagiert sich im BvD als Sprecherin des Arbeitskreises der externen Datenschutzbeauftragten und als Mitglied des Ausschusses Recht & Politik.

PRIVACYSOFT
Datenschutzmanagement as a Service

ENTSCHEIDEND IST DAS WISSEN FÜR MORGEN.

PRIVACYSOFT verfügt über eine integrierte eLearning Plattform über die wir Ihnen Web Based Trainings zur EU-Datenschutz-Grundverordnung anbieten.

Mit diesem optionalen Modul ist es Ihren Mitarbeitenden möglich, selbstständig regelmäßige Sensibilisierungen nach Artikel 39 DS-GVO durchzuführen.

Projekt 29 GmbH & Co. KG | Ostengasse 14
93047 Regensburg | www.privacysoft.de

TEA MUSTAĆ

"DON'T BE SO EMOTIONAL"

Affective Computing under the AI Act and the GDPR

1. Introduction

"When dealing with people, remember you are not dealing with creatures of logic, but with creatures of emotion." Dale Carnegie

The human race has long been fascinated by the role of emotions in our lives. Starting from Aristotle,[1] over 19th century thinkers, such as Charles Darwin and William James,[2] and the scientists in the 1960s, that first imagined machines recognizing human faces,[3] all the way to emotion recognition technologies we discuss today. Over the centuries, our understanding of these "complex experiences of consciousness, bodily sensation, and behaviour"[4] has grown together with the awareness of how these can be manipulated.[5] And now enter artificial intelligence.

Artificial intelligence has given us the possibility to both recognize emotional states and manipulate (not necessarily malevolently) them en mass. Yet, despite centuries of research on emotions and the effect they have on human beings, now coupled with prospects that automation has brought to the fore, our laws oftentimes fall short of granting individuals sufficient protection.[6]

The most recent European legal instrument, the AI Act, ambitiously attempts to rectify this. To assess whether the Act is fit for this task, we will first briefly present the field of affective computing and the questions it raises. Then we will explore the existing pitfalls in protecting individuals against these systems, especially considering the protective framework of the GDPR. Finally, we will illustrate how the AI Act aims to cover the existing gaps as well as what the potential legal implications may be.

2. Affective computing in the legal context

Affective computing was first introduced in a self-published paper by Rosalin W. Picard in 1995, because the technology described in it was disregarded as 'science fiction'.[7] Fast-forward two decades and her once radical claim that "computers [will be able to] read emotions (i.e., infer hidden emotional states based on psychological and behavioral observations)" [8] is not so radical anymore. Quite to the contrary, it underlies a fair number of business models. Many providing tailored, emotion-based marketing and business strategies.[9] Other making our environment more personalized and intuitive, such as smart home devices[10] and cars.[11]

[1] Emotion, Britannica, https://www.britannica.com/science/emotion [accessed on the 3rd of February 2024].

[2] A.S.R. Manstead, 'A history of affect and emotion research in social psychology', Handbook of the History of Social Psychology, edited by A. W. Kruglanski and W. Stroebe, Psychology Press, 2012, p. 177.

[3] Woodrow Bledsoe Originates Automated Facial Recognition, Jeremy Norman's HistoryofInformation.com, https://www.historyofinformation.com/detail.php?id=2126 [accessed on the 3rd of February 2024].

[4] Emotion, Britannica, https://www.britannica.com/science/emotion [accessed on the 3rd of February 2024].

[5] See, for example, S. Schachter and J. E. Singer, 'Cognitive, social, and physiological determinants of emotional state." Psychological review 69, 1962, pp.379-99.

[6] See, for example, A. Häuselmann, 'Fit for purpose? Affective Computing meets EU data protection law', International Data Privacy Law, 2021, Vol. 11, No. 3.; E. Sedenberg and J. C.-I. Chuang, 'Smile for the Camera: Privacy and Policy Implications of Emotion AI', 2017, https://arxiv.org/ftp/arxiv/papers/1709/1709.00396.pdf [accessed on the 3rd of February 2024].

[7] R.W. Picard, 'The Promise of Affective Computing', in Rafael Calvo, and others (eds), The Oxford Handbook of Affective Computing, Oxford Library of Psychology (2015), https://doi.org/10.1093/oxfordhb/9780199942237.013.013 [accessed on the 5th of February 2024].

[8] R. W. Picard, 'Affective Computing', M.I.T Media Laboratory Perceptual Computing Section Technical Report No. 321, 1995, p.9.

[9] For, instance, Cogito AI, https://cogitocorp.com/, Affectiva, https://www.affectiva.com/, Visage Technologies, https://visagetechnologies.com/emotion-recognition/ [accessed on the 5th of February 2024].

[10] See, for example, D. Robitzski, 'AMAZON IS TEACHING ALEXA TO ANALYZE YOUR EMOTIONS – WHAT COULD POSSIBLY GO WRONG?', The Byte, https://futurism.com/the-byte/amazon-alexa-analyzing-emotions [accessed on the 5th of February 2024].

[11] BMW Unveils Color-Changing Car With Emotional Intelligence, Tomorrow's World Today, 9th of January 2023, https://www.tomorrowsworldtoday.com/transportation/bmw-unveils-color-changing-car-with-emotional-intelligence/ [accessed on the 5th of February 2024].

As a result, the once marginal and confusing term now has a firm standing in the scientific literature.[12] One discipline lagging behind, however, is the law.

Namely, besides from obvious cases of manipulation, many affective computing products have much more subtle effects, which will probably not be enough to trigger consumer protection and anti-fraud regulation. What we are then left with is the GDPR, since many of these technologies rely on algorithms extracting patterns from "a variety of measurements including facial expressions, speech, gait patterns and other metrics,"[13] all of which can be considered personal data. However, the GDRP is no longer alone on the frontlines. One other instrument that will have a role to play is the AI Act, that explicitly regulates emotion recognition systems, in general, as well as the use of "polygraphs and similar tools", in particular. One thing that remains unclear is why the Act would not simply regulate affective computing as the term is well established and its scope is broader. Another thing that remains unclear is why the Act would regulate "polygraphs and similar tools" separately. Namely, polygraphs work by measuring "emotional responses to a series of questions" [14] to calculate a deception score, while the AI Act defines emotion recognition systems as "AI systems [used] for the purpose of identifying or inferring emotions or intentions of natural persons" (Article 3(34)), which then clearly covers polygraphs. Furthermore, the AI Act not only confusingly separates the two, but by explicitly mentioning polygraphs it also to an extent acknowledges this pseudoscientific technology. How-ever, to avoid us getting too deep into how things could or should have been, we are instead going to observe them as they are. Therefore, in the next Chapter we will briefly consider the legal implications of the GDPR and the AI Act respectively. As well as uncover some of the persisting gaps in the regulatory framework.

3. Legal assessment

a. GDPR

We have already noted that the goal of affective computing, and emotion recognition as its subset, is to measure physical responses to infer emotional states. It is important to note that although these technologies cannot accurately assess subjective experience, they can estimate emotional responses and general attitude towards external stimuli,[15] for instance, concluding that one movie, song or ad, on average, elicits a more positive reaction than another.[16] And this is enough for them to influence our behavior.

Two important things to separate here are the input to the system and its output. To first focus on the output, emotion recognition systems will usually generate a prediction of a person's mood, general attitude or even specific emotion. These

[12] See, for example, E. Cambria, D. Das, S. Bandyopadhyay, A. Feraco, 'Affective Computing and Sentiment Analysis', in E. Cambria, D. Das, S. Bandyopadhyay, A. Feraco (eds) A Practical Guide to Sentiment Analysis, Socio-Affective Computing, vol 5. Springer (2017) https://doi.org/10.1007/978-3-319-55394-8_1 [accessed on the 5th of February 2024]; J. Han, Z. Zhang, N. Cummins and B. Schuller, 'Adversarial Training in Affective Computing and Sentiment Analysis: Recent Advances and Perspectives [Review Article]' in IEEE Computational Intelligence Magazine, vol. 14, no. 2, pp. 68-81, May 2019, doi: 10.1109/MCI.2019.2901088 [accessed on the 5th of February 2024]; W. Chih-Hung, H. Yueh-Min and Jan-Pan Hwang, Review of affective computing in education/learning: Trends and challenges, BJET, November 2016, Vol. 47, No. 6, pp. 1304-1323.

[13] E. Furey and J. Blue, 'Alexa, Emotions, Privacy and GDPR', 2018, doi: 10.14236/ewic/HCI2018.212 [accessed on the 5th of February 2024].

[14] A. B. Slavkovic, 'Evaluating Polygraph Data' (2002) https://www.stat.cmu.edu/tr/tr766/tr766.pdf pp. 2, 5. [accessed on the 2nd of February 2024].

[15] A. Chen and K. Hao, 'Emotion AI researchers say overblown claims give their work a bad name', MIT Technology Review, 14 of February 2020, https://www.technologyreview.com/2020/02/14/844765/ai-emotion-recognition-affective-computing-hirevue-regulation-ethics/ [accessed on the 2nd of February 2024].

[16] A. Chen and K. Hao, 'Emotion AI researchers say overblown claims give their work a bad name'.

Ratisbona Compliance

DAS HINSCHG IST DA!

Ab 17. Dezember 2023 müssen alle Unternehmen ab 50 Mitarbeitern das Hinweisgeberschutzgesetz (HinSchG) umsetzen.

Das digitale Hinweisgebersystem mit anwaltlicher Expertise der Ratisbona Compliance ist die professionelle Antwort auf die gesetzlichen Anforderungen des HinSchG.

Wir sprechen gerne mit Ihnen darüber, wie wir partnerschaftlich den Hinweisgeberschutz umsetzen können.

FRAGEN SIE AUCH NACH UNSEREN PARTNER-KONDITIONEN

Tel. +49 941 2060384-1

Ratisbona Compliance GmbH | Ostengasse 14
93047 Regensburg | www.ratisbona-compliance.de

outputs might not necessarily be personal, as they are universal and cannot be used to identify a person.[17] Unless, we consider that they are inferences made based on personal data, which might make them just as personal as the original data. The number of arguments for this interpretation is steadily increasing and the game works in both directions. So, for instance, the CJEU decided in Vyriausioji tarnybinės etikos komisija[18] that when dealing with inferences that can be classified as sensitive (e.g. our neural states and reactions can uncover facts about our health, but also our political or other beliefs),[19] the data used to make these inferences respectively deserves the same treatment. Even if it would not be considered sensitive data otherwise. Another way of protecting inferred emotional states relies upon the fact that through the combination of various elements it is still possible to identify the individual (e.g. by linking inferred emotional states and the user profile or the data points used to make the inference), which makes the data personal.[20] So, it is fairly reasonable to conclude that emotions, as inferences made based on sensitive, personal data, are to be classified as personal, if they can in any way and by any whom be traced back to an individual.[21] The question whether the inferred data could be classified as sensitive is admittedly more complex and we will not consider it further at this stage.[22]

On the other hand, in order to make the inference the system will have to process personal data (e.g. facial expressions, gait, speech, etc.), some of which qualifying as special category data. This qualification depends on whether e.g. facial expressions are processed through specific means allowing unique identification of a natural person.[23] This qualifying criterion would then per analogiam also apply to other (potentially) biometric data, such as speech. Therefore, whether the processed data is special category data will have to be assessed on a case-by-case basis, with the AI Act now strengthening the conclusion that it is, by defining emotion recognition systems as systems making inferences based on biometric data. Very important to stress here is that, despite certain actors wanting to apply the same criterion for determining whether the processed data is personal,[24] this argument can never hold ground. The GDPR defines personal data as any information relating to an identified or identifiable natural person. Therefore, it is irrelevant whether a developer of an emotion recognition system also identifies the person, it is only relevant whether he can theoretically do so. Yet, despite this being the case, many of these technologies and their providers fail to comply with the GDPR's obligations, especially those concerning lawfulness and transparency.[25] This means that the data subjects are exposed to these systems, often being completely unaware of the fact.

Therefore, we can conclude that even though the GDPR theoretically provides protection to affected persons, it fails to do so in an efficient manner. But all is not yet lost, maybe the AI Act will do something to rectify the situation and provide the much-needed protection.

b. AI Act

The AI Act deals with the question of affective computing, regulating it in at least three specific instances: emotion recognition systems in education and at work, emotion recognition systems in all other contexts, and "polygraphs and similar tools" used in law enforcement, migration, asylum and border management. Consequently, there are certain obligations that apply to these three categories respectively.

[17] A. Hauselmann, A. M. Sears, L. Zard, and E. Fosch-Villaronga, 'EU law and emotion data', 11th International Conference on Affective Computing and Intelligent Interaction (ACII), 2023, p.3.

[18] Judgment from the 01 of August 2022 Vyriausioji tarnybinės etikos komisija C-184/20, ECLI:EU:C:2022:601.

[19] M. Ienca and G. Malgieri, 'Mental data protection and the GDPR', Journal of Law and the Biosciences, p.7, https://doi.org/10.1093/jlb/lsac006 [accessed on the 6th of February 2024].

[20] M. Ienca and G. Malgieri, 'Mental data protection and the GDPR', Journal of Law and the Biosciences, p.8.

[21] See, for example, Opinion 216/679, adopted on 3 October 2017, revised in 6 February 2018., European Parliamentary Research Service Scientific Foresight Unit, Panel for the Future of Science and Technology, 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence', (STOA) PE 641.530, June 2020, ICO Guidance for the use of personal data in political, https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guidance-for-the-use-of-personal-data-in-political-campaigning-1/personal-data/#opinions [accessed on the 5th of February 2024].

[22] For an extensive discussion see, M. Ienca and G. Malgieri, 'Mental data protection and the GDPR'.

[23] Recital 51 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[24] N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', Vol. 10 No. 1 Law, Innovation and Technology (2018) pp. 40, 74-75, https://www.tandfonline.com/doi/full/10.1080/17579961.2018.1452176 [accessed on the 2nd of February 2024]; A. McStay, 'Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy', Big Data & Society January–June 2020: 1–12, DOI: 10.1177/2053951720904386.

[25] See, for example, A. McStay, 'Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy'.

The first recon with emotion recognition in education and at work, these systems are in general prohibited (Article 5), unless used for medical or safety reasons. The supposed reason for this prohibition is that "considering the imbalance of power in the context of work or education, combined with the intrusive nature of these systems, such systems could lead to detrimental or unfavourable treatment of certain natural persons or whole groups thereof."[26] Unfortunately, the Act does not clarify why this power imbalance, intrusive nature and potentially discriminatory effects justify a prohibition only in these two contexts. It also does not clarify what medical and safety reasons might still justify their use. These are all questions that will have to be answered once the Act is in force.

The second category, including the use of "polygraphs and similar tools" in law enforcement, migration, asylum and border control is classified as high-risk. Firstly, as already pointed out, it is completely unclear why the Act describes these systems rather than using the same "emotion recognition" terminology. Secondly, both Recital 38 and 39 acknowledge that the use of these systems in the said contexts is associated with a significant degree of power imbalance due to the vulnerability of the people affected by the technology. And yet this does not seem to justify their prohibition. Thirdly, the Recitals acknowledge possible effects of low-quality training data, lack of transparency and accountability on affected persons, yet the use of these systems in law enforcement is excluded from transparency obligations (Article 52(2)). And the systems used in both mentioned contexts must only be registered in a "secure, non-public section of the EU database" (Article 51(1c)). So not only does the "significant power imbalance" in these contexts not merit prohibition, but it apparently does not merit even the basic requirements of transparency. The only straw to grasp on here is Recital 41, which states that "the fact that an AI system is classified as a high-risk AI system … should not be interpreted as indicating that the use of the system is lawful under other acts of Union law or under national law." So, at least the member states that forbid the use of such systems, such as for instance Germany where the use of polygraph in court and criminal investigations has been forbidden since 1954,[27] can continue to protect their citizens from their pseudoscientific outputs.

The third category, including emotion recognition sys-

[26] Recital 26c of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021/0106(COD), 26th of January 2024.

[27] See Urteil des BGH vom 16.02.1954, Az. 1 StR 578/53, https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=16.02.1954&Aktenzeichen=1%20StR%20578%2F53 [accessed on the 3rd of February 2024].

tems used in all other context, is also classified as high-risk without any apparent exceptions. Of course, there always remains a possibility for a developer to claim that a particular system is not high-risk as it poses no risk of significant harm to life, health or other fundamental rights (Article 6(2)). However, this will probably be a high threshold to meet considering the power of these technologies and will still have to be reported to the authorities. In the event that the threshold is not met, the AI Act will impose some stringent requirements that will have to be built into the system. These include designing and running risk and quality management systems, including the possibility of human oversight, mandatory registration and documentation obligations, as well as automated logging and record keeping. Finally, Article 52(2) explicitly mandates increased transparency towards the persons affected by these systems as well as honoring the existing data protection regulations. These obligations are by no means trivial, especially considering that many of such systems, including e.g. smart billboards, emotion-tailored content recommendations, etc., often commence processing operations as soon as an individual is in the proximity of the system.

Finally, there is one more instance of somewhat hidden regulation of emotion recognition systems, this time in the context of accessing public services. Namely, Annex III (5)(c), classifies "AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in the dispatching of emergency first response services" as high-risk. Evaluating and classifying emergency calls to establish priority can hardy occur without speech pattern analysis, in much of the same way as today's biggest companies deploy emotion recognitions speech analysis to customer service calls to determine who should have priority.[28] In the emergency call context, however, it is disturbingly easy to see how this can lead to unjust outcomes. For example, some criteria for call redistribution include recognized states of fear and anxiety, that may lead to the classification of calls as more urgent.[29] What this can lead to is that a caller experiencing a more urgent situation but sounding calmer can have increased waiting time over a person in a less urgent situation but prone to panicking. The only thing making the situation even worse is the brain gymnastics exercise we need to conduct to reach this conclusion and consider the implications of this provision.

4. Conclusion

The AI Act is far from being the magical solution to all the questions and legal loopholes that the GDPR left in the regulation of emotion recognition systems. Furthermore, the Act still leaves wide gaps, especially when the deployment of these technologies by public authorities and the police are concerned. However, when it comes to commercially deployed emotion recognition systems the Act is bound to close at least some of the existing legal gaps.

Finally, even though some of the obligations under the Act are a force to be reckoned with and will have to be considered from the very start of the developmental process, in the end, the protection achieved will always come down to enforcement. Due to the inherently invisible character of these systems, enforcing the introduced obligations will be a challenge in its own right. We can only hope that the market surveillance authorities tasked with monitoring the adherence to the Acts obligations will be up to the task.

Über die Autorin

Tea Mustać
ist eine Rechtswissenschaftlerin und Expertin für Datenschutz sowie geistiges Eigentum bei der Spirit Legal Rechtsanwaltskanzlei. Sie berät Unternehmen beim Einsatz von Technologien und verfasst Beiträge zu einer Vielzahl von Themen an der Schnittstelle zwischen Recht und Technologie, mit einem besonderen Schwerpunkt auf Künstlicher Intelligenz. Darüber hinaus hält sie regelmäßig Seminare zu KI und Data Governance an der BeckAkademie und moderiert den Podcast RegInt: Decoding AI Regulation.

[28] One example of a tool for establishing calling priority within customer service is Sprinklr Service. For more, see https://www.sprinklr.com/help/articles/how-to-setup-business-logic/how-to-prioritise-certain-customer-calls/647c38aa723d925979db78c7 [accessed on the 3rd of February 2024].

[29] See, for example, M. Bojanić, V. Delić, and A. Karpov, 'Call Redistribution for a Call Center Based on Speech Emotion Recognition', Appl. Sci. 2020, Vol. 10, p. 4653. https://doi.org/10.3390/app10134653 [accessed on the 3rd of February 2024].

+++ Hybrid-Veranstaltung: Teilnahme vor Ort sowie Online möglich! +++ Anzeige

Datenschutzkonferenz 2024

Praxis | Recht | Innovation

11. - 13. September 2024 | Hotel Kö59 Düsseldorf

September 2024						
Mo	Di	Mi	Do	Fr	Sa	So
						1
2	3	4	5	6	7	8
9	10	**11**	**12**	**13**	14	15
16	17	18	19	20	21	22
23	24	25	25	25	25	25
30						

Sichern Sie sich den **Frühbucherrabatt** auf Ihre Preiskategorie und melden sich frühzeitig an!

Anmeldeschluss: 10.09.2024
Eine frühzeitige Anmeldung wird empfohlen.

Teilnahmegebühr (zzgl. MwSt.)*:
a) 1.049,– EUR für **Behördenvertreter**
b) 1.149,– EUR für **Abonnenten** des „Datenschutz-Berater“, „Compliance-Berater“ und „Kommunikation & Recht“
c) 1.599,– EUR Normalpreis

Rabatte – so sparen Sie intelligent (zzgl. MwSt.):
Frühbucherrabatt: 50,– EUR bei Anmeldung bis zum 15.03.2024 auf alle Preiskategorien
Mehrbucherrabatt: 5 % bei Anmeldung von mehr als 3 Teilnehmern einer Kanzlei/eines Unternehmens ab dem 3. Teilnehmer (unabhängig vom Frühbucherrabatt)

Veranstaltungsort:
Hotel Kö59 Düsseldorf, Königsallee 59, 40215 Düsseldorf

Anmeldung:
Herrn Jasha Baniashraf, Deutscher Fachverlag GmbH,
Mainzer Landstraße 251, 60326 Frankfurt am Main
Telefon: 069/7595-2773
E-Mail: Jasha.Baniashraf@dfv.de

Stornierung/Übertragung:
- Die Anmeldung ist übertragbar.
- Bei Stornierung bis 28 Tage vor Veranstaltung *(Eingangsdatum)* wird eine Bearbeitungsgebühr i.H.v. 75,– EUR erhoben. Danach sowie bei Nichterscheinen eines Teilnehmers ist die volle Teilnahmegebühr zu entrichten.

**Der Preis schließt Veranstaltungsunterlagen, die Pausenverpflegung und die Abendveranstaltungen mit ein. Die Teilnahmegebühr bitten wir erst nach Erhalt der Rechnung zu überweisen. Eine Teilnahmebestätigung wird erteilt.*

Anmeldung zur Datenschutzkonferenz 2024 – Düsseldorf

auf www.datenschutzkonferenz.de | per Fax an: 069. 75 95 - 1150 | per E-Mail: Jasha.Baniashraf@dfv.de

Kanzlei/Firma: _____

Name, Vorname: _____

Straße, Nr.: _____

PLZ, Ort: _____

Tel.: _____ E-Mail: _____

DSB, K&R und CB Kundennummer: _____

Datum: _____ Unterschrift: _____

☐ **Teilnahme vor Ort** ☐ **Teilnahme online**

Ich nehme am Vorabendempfang (Mi) teil: ja ☐ nein ☐

Ich nehme am Abendessen (Do) teil: ja ☐ nein ☐

☐ **a) Behördenvertreter**
☐ **b) Abonnent des DSB, CB oder K&R**
☐ **c) regulärer Preis**

Sie haben den DSB, K&R und CB noch nicht im Abo?

☐ Ja, ich möchte den DSB – „Datenschutz-Berater“ zum Jahresbezugspreis Inland **379,– EUR** abonnieren.

☐ Ja, ich möchte den CB – „Compliance-Berater“ zum Jahresbezugspreis Inland **589,- EUR** abonnieren.

☐ Ja, ich möchte die K&R – Zeitschrift für „Kommunikation & Recht“ zum Jahresbezugspreis Inland **584,– EUR** abonnieren.

Alle Zeitschriftenpreise inkl. Vertriebskosten und MwSt. Lieferung ab sofort.

Medienpartner:

DATENSCHUTZ-BERATER | Compliance Berater | Kommunikation & Recht

Eine Veranstaltung der dfv Mediengruppe

GERHARD FRIEDERICI

KEINE CHANCE FÜR LANGE FINGER?

Der Zugriffsschutz als wesentlicher Sicherheitsaspekt in der Lagerung und Entsorgung vertraulicher Informationsträger – Technik und Methoden

Ob Papierakte, CD, USB-Stick oder Festplatte – die lokalen Aufbewahrungs- und Speichermöglichkeiten für Informationen sind vielfältig, wenn nicht unüberschaubar. Der Schutz der in diesen Informationen abgebildeten Daten, insbesondere, wenn diese personenbezogener oder sonst schutzwürdiger Natur sind, stellt Unternehmen wie auch Einzelpersonen vor besondere Herausforderungen. Durch den Einsatz spezieller technischer Lösungen, als Ergebnis einer durchdachten Produktkonzeption unter Beachtung des Grundsatzes „Privacy-by-Design", lässt sich der Zugriffsschutz verbessern und können Fehlerquellen wie beispielsweise menschliches Versagen ausgeschaltet werden.

Neben einem Eigeninteresse der verantwortlichen Stelle für den Schutz der für die eigene Arbeit wertvollen Daten kommt die zunehmende Regelungsintensität durch nationale und transnationale Stellen mehr und mehr zum Tragen. EU-Verordnungen und -Richtlinien werden in den nächsten Jahren Datenschutz und Cybersicherheit noch stärker als bisher regulieren und damit neue Anforderungen für die verantwortlichen Stellen formulieren.

Zugriffsschutz im Büroalltag

Im modernen Büroalltag entstehen umfangreiche Datenmengen bereits durch die Abwicklung der regulären Arbeitsprozesse. Die Anlage von Kundenkonten, der Aufruf von Patientendaten oder die Erstellung von Dokumenten produzieren zu verwaltende und in aller Regel auch zu schützende Datenpunkte. Vielen ist die Sensibilität dieser Informationen und die möglichen schwerwiegenden Auswirkungen eines Missbrauchs nicht ausreichend bewusst. Durch Unwissen, Sorglosigkeit oder böswilliges Handeln stellt der Faktor Mensch hier ein erhebliches Sicherheitsrisiko dar, von der Erstellung über die Archivierung bis hin zur Entsorgung vertraulicher Informationen.

Sichere Lagerung für Informationsträger – Schublade, Schrank, Schlüssel

Durch geordnete Ablage und Unterbringung in verschlossenen Lagerorten wie Aktenschränken können Informationsträger wirksam vor dem unbefugten Zugriff Dritter geschützt

werden. Eine simple Maßnahme wie das Abschließen des Büros beim Verlassen erhöht die Hindernisschwelle für Innen- und Außentäter bereits spürbar.

Computerarbeitsplätze und andere elektronische Arbeitsgeräte können mit einem sicheren Kennwortschutz versehen vor unbefugter Nutzung geschützt werden – durch automatische Sperrung bei Inaktivität kann man hier bereits einen Sicherheitsgewinn erzielen. Dies ist aufgrund der immensen Datendichte eines modernen Computers und Datenträgers dringend notwendig, ebenso wie der Schutz von Ports, die Verschlüsselung mobiler Datenträger, sofern diese überhaupt genutzt werden – denn USB-Sticks und tragbare Festplatten stellen für sich bereits bedeutende Schwachstellen dar, sodass deren Einsatzmöglichkeiten einer Risikoabwägung unterzogen werden sollten.

Zugriffsfreie Vernichtung am Dokumentenlebensende – wie organisieren?

Doch was ist mit nicht mehr aufbewahrungspflichtigen Unterlagen oder Daten, bezüglich derer der Zweck der Datenspeicherung erloschen ist? Die Entsorgung beispielsweise von Aktenordnern über den Papiermüll ist de facto auszuschließen, da man immer davon ausgehen muss, dass ein Ordner auch besonders schutzwürdige Informationen enthält und Dritte diese unbefugt verwenden. In den vergangenen Jahrzehnten hat sich auf diesem Grundgedanken auch in Deutschland eine Branche aus Vernichtungsdienstleistern etabliert, die in unterschiedlicher Flächenabdeckung und mit verschiedenen Prozessen die Sammlung und Vernichtung von Unterlagen, aber auch Datenträgern für ihre Kunden, vom KMU über den Großkonzern bis hin zu Behörden und anderen öffentlichen Stellen organisieren.

Die DIN 66399 dient hier als Industriestandard für strukturierte, sichere Prozesse und technische wie organisatorische Maßnahmen.

Grundlagenexkurs: Der typische Ablauf der Vernichtung von Informationsträgern

Gemeinsam ist diesen Dienstleistungen üblicherweise die Gestellung von Sammelbehältern verschiedener Art, von Konsolen mit Abfallsäcken über Kunststoffbehälter mit Vorhängeschlössern bis hin zur Rollcontainern aus Leichtmetall mit integrierten mechanischen oder elektronischen Schließmechanismen, auch in Verbindung mit weiteren Voraussetzungen (etwa eine Überwachung des Neigungswinkels zur Bewegungserkennung).

Die verantwortliche Stelle sammelt die zu vernichtenden Unterlagen in diesen Behältern und beauftragt die Abholung voller Behälter durch den Dienstleister.

Die Abholung kann, analog zur Abholung der (für schutzwürdige Unterlagen ungeeigneten!) „Altpapiertonne", turnusmäßig erfolgen. Doch durch den oft unregelmäßigen Anfall der Materialmengen wie auch das aufgrund der Aufwendungen für Personal, Technik und Prozesse erhöhte Kostenniveau werden oftmals bedarfsgesteuerte Abholmodelle vereinbart. Hier prüfen zum Beispiel Angestellte des Betriebes in mehr oder weniger regelmäßigen Abständen den Füllstand des Behälters, um zum angemessenen Zeitpunkt einen Auftrag zur Abholung zu erteilen.

Nach Abholung wird der Behälter zu einem Vernichtungsstandort transportiert, dort in einem durch die DIN 66399 definierten Sicherheitsbereich geöffnet und entleert. Anschließend wird das Material in geeigneten Anlagen geschreddert. Für Material der Schutzklasse 3 sind entweder besondere, zugriffsgeschützte Maschinen oder Mobilvernichtungsfahrzeuge einzusetzen, da hier ein ununterbrochener Zugriffsschutz während des Transports und der Vernichtung sichergestellt werden muss.

Allerdings birgt dieses Modell grundsätzliche Risiken, da der Zugriff auf den Behälterinhalt erforderlich ist – die prüfende Person muss den Behälter öffnen und einsehen. Die innerbetrieblichen Zugriffsbeschränkungen beim Kunden wie beim Dienstleister müssen zusätzlich beachtet werden.

Wird der Behälter nach der Inspektion nicht wieder ordnungsgemäß verschlossen, kann ein unbefugter Zugriff durch Dritte erfolgen. Zudem steht und fällt das Modell mit der Vertrauensposition, die die prüfende Person innehaben muss, und stellt damit zusätzliche Anforderungen an das Personalmanagement und die Organisationsstruktur.

Wird die Abholung der im Büro anfallenden Fraktionen (einschließlich der schutzwürdigen Unterlagen) durch einen Facility-Management-Dienstleister organisiert und gesteuert, kommt der Drittenstatus erschwerend hinzu und muss im Datenschutzkonzept des Kundenunternehmens berücksichtigt werden.

Neben diesem unmittelbaren Sicherheitsrisiko durch den nicht ununterbrochenen Zugriffsschutz kommt als weiterer Aspekt die Frage der Entsorgungsverfügbarkeit hinzu. Wird der Sammelbehälter nicht rechtzeitig beauftragt und/oder geleert, zum Beispiel, weil die Prüfung und damit die Bestellung sich verzögerten, kann der Behälter vor Abholung bereits so stark gefüllt sein, dass eine weitere Befüllung durch Mitarbeitende des Kundenbetriebs nicht möglich ist. Menschen sind Menschen – man kann nicht sicher sein, dass alle Mitarbeitenden dann ihre zu vernichtenden Unterlagen wieder mitnehmen und nicht einfach auf dem Behälter liegen lassen – „es wird ja schon passen".

Wie kann man dieser Problematik begegnen? Eine Möglich-

keit ist die stringente Umsetzung eines kurzen Prüfintervalls. Dabei überprüft eine Person den Füllstand täglich oder mehrmals pro Woche. Dies löst jedoch nicht das Problem des für die Prüfung unterbrochenen Zugriffsschutzes und der nicht ordnungsgemäßen Schließung des Behälters danach. Zudem ist ein solches Modell gerade bei größeren Organisationseinheiten mit enormem Zeitaufwand und entsprechenden Kosten verbunden – gerade im öffentlichen Sektor oder bei Versicherungen und Finanzunternehmen können an einzelnen Verwaltungsstandorten durchaus dreistellige Behälterzahlen vorhanden sein. Technische Maßnahmen sind organisatorischen oder persönlichen immer vorzuziehen.

Technische Maßnahmen als Lösungsansatz

Es ist also naheliegend, die Prüfung nicht durch organisatorische, sondern technische Maßnahmen zu erleichtern beziehungsweise abzulösen. Der grundlegende Ansatz ist, den Behälter selbst eine Prüfung vornehmen zu lassen. Dies erfolgt über eine geeignete Sensorik, mit der der Behälter auszustatten ist.

Denkbar sind hier zum einen gewichtssensitive Platten am Behälterboden, die bei Erreichen eines gewissen vordefinierten Füllgewichts einen Alarm auslösen. Hier besteht jedoch das Risiko, dass das eigentliche Füllvolumen gar nicht erreicht wird, zum Beispiel bei Befüllung mit unerwartet schweren Inhalten, und daher unnötige Kosten bei einer zu früh beauftragten Abholung entstehen. Hinzu kommt die kontinuierliche mechanische Belastung des Wiegesensors durch aufliegendes Material und beim Einwurf einwirkende Punktkräfte.

Durch den technischen Fortschritt sind auch Kamerasensoren möglich und bezahlbar geworden, doch hier besteht das signifikante Risiko, dass enthaltene Inhalte erkannt und ausgelesen werden können. In Verbindung mit möglichen Sichtblockaden durch unglücklich fallende Inhalte muss diese Methode damit für sensible Informationsträger ausgeschlossen werden.

Eine weitere und vielversprechende Methode, die bereits in verschiedenen Industriebranchen eingesetzt wird, ist die Messung der Inhalte durch Lasersensorik. Hier tastet ein eingebautes Sensormodul in regelmäßigen Abständen den Behälterinhalt ab und erfasst die Füllhöhe des vorhandenen Materials. Bei Erreichen des vordefinierten Füllstandes wird der Abholalarm ausgelöst. Die wesentlichen Vorteile sind hierbei, dass der Sensor erheblich geringeren Belastungen ausgesetzt ist, nur in Abständen aktiv wird und damit weniger Energie verbraucht, keine Inhalte erfasst und primär das Volumen prüft – natürlich bedeutet dies eine Empfindlichkeit gegenüber besonders raumgreifenden Inhalten, doch ist der Behälter beispielsweise mit einem Einwurfschlitz mit Federklappe ausgestattet, können nur Loseblätter und flexible Mappen eingefüft werden. Damit wird der zur Verfügung stehende Raum weitgehend ausgenutzt.

Wie gelangen nun die erhobenen Informationen zum Dienstleister? Denkbar ist, den Status des Behälters durch Signalleuchten am Behälter sichtbar zu machen: Ein grünes Licht zeigt „verfügbar", ein gelbes Licht „abholbereit" und ein rotes Licht „gefüllt und nicht verfügbar" an. Hierbei muss aber immer noch eine Person die Behälter überprüfen, den jeweiligen Status vermerken und tätig werden. Somit ist nur der Zugriffsschutz durch den Wegfall der notwendigen Öffnung für die Prüfung verbessert, operativ handelt es sich immer noch um ein personalintensives Modell.

Damit ist es naheliegend, auch die Alarmmeldung zu automatisieren; eine drahtlose Übertragungslösung bietet sich an. Ein entsprechendes Sensormodul umfasst neben dem eigentlichen Sensor, einem Mikrocontroller und einer Energieversorgung dann auch einen Signaltransmitter oder -transceiver. Als Stand der Technik kann hier 5G-Technologie zum Einsatz kommen. Die Kommunikationen sind selbstverständlich zu verschlüsseln, geeignete und im Alltagsgebrauch sichere Verschlüsselungsmethoden existieren. Die Information wird an eine empfangende Stelle übermittelt und stößt dort den entsprechenden Abwicklungsprozess an. Grundsätzlich sollte die Datenübertragung nur ein Minimum der erforderlichen Daten umfassen, wie eine eindeutige Behälter-Identifikationsnummer, den Messzeitpunkt und den Füllstand, so dass ein möglicher Angreifer keine Rückschlüsse auf den Standort und die Identität des Kunden ziehen kann; diese Informationen sind lediglich als notwendige Kundenstammdaten im ERP-Sys-

tem des Dienstleisters gespeichert und werden dort, durch wirksame informationstechnische Sicherheitsmaßnahmen geschützt, für die Zwecke der Abholungsdisposition zusammengeführt.

Auch auf diesem Prozessschritt sind Automatisierung und Integration in bestehende Informationsnetzwerke wünschenswert, was auf eine Anbindung des Sensors an ein vorhandenes Unternehmensnetzwerk oder eine cloudbasierte Onlinelösung hinausläuft – hier muss dann besonderes Augenmerk auf hochwertige SSL- oder TLS-Verschlüsselungen des laufenden Datenverkehrs gelegt werden, um Angriffen vorzubeugen. Zwar überträgt der Lasersensor selbst keine vertraulichen Daten aus den Behälterinhalten, doch muss auch die Möglichkeit ausgeschlossen werden, dass sich ein Angreifer über die Verbindung Zugang zum Unternehmensnetzwerk und dort gespeicherten Informationen verschafft.

Nach Eingang der Sensorinformationen in der Verwaltungsanwendung können verschiedene berechtigte Akteure diese Informationen einsehen und entsprechende Maßnahmen treffen. Ein Facility Manager am Standort kann damit beispielsweise eine Bestellung beim Dienstleister aufgeben, die betroffenen Behälter zum nächstmöglichen Zeitpunkt zu wechseln.

Wird der Sensor durch den Dienstleister als Teil des Service bereitgestellt, so erhält auch dieser bereits die für den Zweck der Abholplanung und -umsetzung erforderlichen Informationen mit der Sensormeldung und kann bereits einen provisorischen Auftrag einplanen. Die Übertragung personenbezogener Daten ist, wie oben beschrieben, hierfür nicht erforderlich – nach einmaliger Anlage der relevanten Stammdaten im System des Dienstleisters müssen diese lediglich in der geschützten Umgebung des ERP-Systems verarbeitet werden.

Perspektivisch ist es auch möglich, den Nachweis der Zuverlässigkeit des Sensors vorausgesetzt, eine automatische Beauftragung bei Erreichen des Abholfüllstands vertraglich zu vereinbaren und technisch einzurichten. Hierdurch kann weiterer manueller Arbeitsaufwand eingespart werden.

Sollte eine Organisationseinheit für die Vernichtung vertraulicher Datenträger und Unterlagen nicht auf einen externen Dienstleister setzen, sondern dies in Eigenregie vornehmen, sind Sensoren auch für die eigene Nutzung zu erwerben und nicht zwingend an einen Dienstleister gebunden. Hierbei sind die Anforderungen an die eigene IT-Sicherheit, eigene Organisations- und Prozessstrukturen und der notwendige Umsetzungsaufwand zu berücksichtigen, doch lässt sich diese Art von Füllstandssensoren auch für eine Vielzahl anderer zugriffsfreier Inhaltsüberwachungszwecke einsetzen. Der Aufwand für eine Umsetzung in Eigenverantwortung ist damit jedoch nicht unbeträchtlich und sollte unbedingt in die vollständige Abwägung einfließen.

Dieses automatisierte Modell aus Lasersensor und drahtloser Informationsübertragung vereinbart bei korrekter Umsetzung verschiedene wünschenswerte Effekte:

- einen erhöhten Zugriffsschutz durch den Wegfall unnötiger Behälteröffnungen;
- schnelle Reaktionszeiten durch die Straffung des Erfassungs- und Bestellprozesses;
- kontinuierliche Verfügbarkeit des Sammelbehälters durch rechtzeitige Leerung.

Zusammenfassend lässt sich feststellen:

Der klassische Vernichtungs- und Entsorgungsprozess für sensible Informationsträger weist an vielen Punkten Schwachstellen auf, die im Wesentlichen auf den Faktor Mensch und die Abweichung von etablierten organisatorischen Maßnahmenvorgaben zurückzuführen sind.

Durch die konsequente Umsetzung existierender technischer Maßnahmen lassen sich hier eindeutige Sicherheitsgewinne realisieren. Die kontinuierlich sinkenden Implementations- und Transaktionskosten für solche integrierten Systemlösungen machen die Einführung einer „schlüsselfertigen" Sensorlösung vom zertifizierten Dienstleister nicht nur für große Organisationen, sondern auch bereits für mittlere Unternehmensgrößen attraktiv.

Die technische Lösung mit einer Füllstandssensorik für Sicherheitsbehälter ist aufgrund der genannten Effekte aus datenschutzrechtlicher Sicht den organisatorischen Maßnahmen eindeutig vorzuziehen, da die Datensicherheit erhöht und das Risiko „Mensch" minimiert wird.

Über den Autor

Gerhard Friederici
ist Datenschutzbeauftragter in der Rhenus-Gruppe und leitet das Service Center Corporate Privacy & Quality, Health, Safety, Environment der Rhenus Office Systems GmbH. Er ist im Vorstand des bvse-Fachverbands Akten- und Datenträgervernichtung, Mitglied im Arbeitskreis Datenschutzgerechte Datenträgerentsorgung nach dem Stand der Technik der GDD e.V., sowie Mitglied im DIN Normenausschuss NA 043-01-51 Vernichten von Datenträgern. Als Referent tritt Gerhard Friederici zu den Themenfeldern Compliance und Datenschutz auf.

▶ www.office-systems.de

DATENSCHUTZRECHTLICHE HERAUSFORDERUNGEN DER VERWALTUNGSDIGITALISIERUNG

Katja Horlbeck

Datenschutzrechtliche Herausforderungen der Verwaltungsdigitalisierung

Leicht kann der Eindruck entstehen, dass Beratung, Überwachung, Einhaltung und Durchsetzung datenschutzrechtlicher Vorschriften gegenüber nicht-öffentlichen Stellen im Fokus der aufsichtsbehördlichen Tätigkeit stehen. Ein Blick in die Arbeitsstatistik der Datenschutzaufsichtsbehörden zeigt aber, dass ein wesentlicher Teil der Arbeitskraft auch durch die Behandlung datenschutzrechtlicher Fragestellungen aus dem öffentlichen Bereich gebunden wird.[1]

Besondere Bedeutung kommt hier beispielsweise Sachverhalten zu, die sich den Begriffen „Verwaltungsmodernisierung und Verwaltungsdigitalisierung" zuordnen lassen. Ziel der Verwaltungsmodernisierung ist es Verwaltungsprozesse zu straffen und zu optimieren, Bürgerinnen und Bürgern sowie Unternehmen medienbruchfreie Serviceleistungen zur Verfügung zu stellen und die Zusammenarbeit zwischen öffentlichen Stellen zu vereinfachen.[2] Zentrales Instrument der Verwaltungsmodernisierung ist dabei die Digitalisierung des Verwaltungshandelns, etwa durch die Einführung und Nutzung elektronischer Aktenführungssysteme sowie des elektronischen Behördenpostfachs oder durch die Bereitstellung von Verwaltungsleistungen über das Internet.

Auch wenn eine schnellere, effektivere und nutzerfreundlichere Verwaltung vollumfänglich zu begrüßen ist: Öffentliche Stellen sind hierbei an die Vorgaben des Datenschutzrechts in gleicher Weise gebunden wie nicht-öffentliche Stellen. Daneben besteht ein originäres Interesse an einer datenschutzkonformen Verwaltungsdigitalisierung, denn diese schafft Vertrauen und Akzeptanz auf Seiten der nutzenden Bürgerinnen und Bürger und ist somit ein wesentlicher Erfolgsfaktor.[3]

Onlinezugangsgesetz als rechtliches Fundament der Verwaltungsdigitalisierung

Soweit es den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern betrifft (d. h. die Bereitstellung von Verwaltungsleistungen über das Internet), bilden Art. 91c Abs. 5 Grundgesetz (GG) und das Onlinezugangsgesetz (OZG) das rechtliche Funda-

[1] Einundfünfzigster Tätigkeitsbericht zum Datenschutz und Fünfter Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, 295, https://datenschutz.hessen.de/infothek/taetigkeitsberichte, zuletzt abgerufen am 21.02.2024.

[2] BMI, https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/verwaltungsmodernisierung-node.html, zuletzt abgerufen am 21.02.2024.

[3] Einundfünfzigster Tätigkeitsbericht zum Datenschutz und Fünfter Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, 91 ff., https://datenschutz.hessen.de/infothek/taetigkeitsberichte, zuletzt abgerufen am 21.02.2024.

ment der Verwaltungsdigitalisierung.[4] Das 2017 verabschiedete OZG verpflichtet Behörden Verwaltungsleistungen, wie z. B. den Antrag auf Eheschließung oder auf Erteilung einer Fahrerlaubnis, digital über Verwaltungsportale anzubieten.[5]

Nach dem OZG-Umsetzungskonzept des Bundesministeriums des Innern, für Bau und Heimat (BMI) von 2018 sollten auf der Grundlage des OZG bis zum 31.12.2022 etwa 575 OZG-Leistungen umgesetzt werden.[6] Dieses Ziel konnte nicht erreicht werden. Bereits 2022 begannen nicht zuletzt auch aus diesem Grund die Arbeiten an einer Änderung des OZG. Im Januar 2023 wurde sodann ein Referentenentwurf vorgelegt und im Mai 2023 folgte der Gesetzesentwurf der Bundesregierung. Am 23.02.2024 hat der Bundestag dem Gesetzesentwurf zur Änderung des OZG zugestimmt.[7] Nach der Verabschiedung im Bundestag bedarf es nun noch der Zustimmung im Bundesrat.

Die Digitalisierung von etwa 575 Verwaltungsleistungen mag auf den ersten Blick möglicherweise nicht besonders kompliziert oder gar überschaubar erscheinen. Wird aber berücksichtigt, dass der Großteil der Verwaltungsleistungen durch die Bundesländer und die knapp 11.000 Kommunen erbracht werden, ergibt sich eine erhebliche Anzahl erforderlicher Umsetzungsprojekte. So ging der Nationale Normenkontrollrat im Oktober 2019 in einer groben Überschlagsrechnung von etwa 180.000 Implementierungen aus.[8] Die Umsetzung des OZG ist damit das größte Modernisierungsvorhaben der Bundesrepublik seit ihrem Bestehen.[9]

Verwaltungsdigitalisierung nach dem EfA-Prinzip

Um diese Herkulesaufgabe überhaupt realisieren zu können, wurde das sogenannte „Einer für Alle“ (EfA)-Prinzip entwickelt. Dem EfA-Prinzip liegt der Gedanke einer effizienten, nachhaltigen und kostenschonenden Verwaltungsdigitalisierung durch interföderale Kooperation zugrunde.[10] Es besteht aus vier wesentlichen Schritten: (1) Ein Land A digitalisiert eine Verwaltungsleistung (Onlinedienst) zentral in einem einheitlichen Design, (2) ein Dienstleister B betreibt die für den Onlinedienst erforderliche IT zentral, (3) alle übrigen Länder bzw. Kommunen (nachnutzende Länder und Kommunen C) nutzen den von Land A entwickelten und von dem Dienstleister B betriebenen Onlinedienst nach, schließlich wird (4) der Onlinedienst zentral für alle Länder weiterentwickelt und der Betrieb anteilig finanziert.[11]

Datenschutzrechtliche Herausforderungen des EfA-Prinzips

Auch wenn die Umsetzung des OZG nach dem EfA-Prinzip sinnvoll ist: Mit Blick auf das Datenschutzrecht birgt die Digitalisierung von Verwaltungsleistungen nach dem EfA-Prinzip einige Herausforderungen. So stellt sich beispielsweise die Frage der datenschutzrechtlichen Verantwortlichkeit i. S. v. Art. 4 Nr. 7 DS-GVO. Zu klären ist etwa wie die datenschutzrechtlichen Rollen der beteiligten Akteure (Land A, Dienstleister B, nachnutzende Länder und Kommunen C) zu bewerten sind, welche Verantwortlichkeiten im Sinne der DS-GVO (Verantwortlichkeit, gemeinsame Verantwortlichkeit oder Auftragsverarbeitung) entstehen und wie die hieran anknüpfenden Rechtsfolgen effizient realisiert werden können (bedarf es der Schaffung neuer gesetzlicher Grundlagen oder sind zahlreiche Verträge abzuschließen).[12] Dem Grundsatz der Rechtmäßigkeit des Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 DS-GVO folgend muss zudem die Frage geklärt werden, welche Rechtsgrundlagen für die unterschiedlichen Datenverarbeitungen, die mit der Nutzung eines Onlinedienstes einhergehen, zur Anwendung gelangen. Die fachlich zuständige Behörde des nachnutzenden Landes/der nachnutzenden Kommune C kann die Verarbeitung personenbezogener Daten für die Inanspruchnahme der Verwaltungsleistung in der Regel auf Art. 6 Abs. 1 UAbs. 1 Buchst. e i. V. m. Art. 6 Abs. 3 i. V. m. einer Vorschrift aus dem jeweils einschlägigen Fachrecht stützen. Es fehlen aber Rechtsgrundlagen für Datenverarbeitungen, die der Bearbeitung der fachlich zuständigen Behörde vorgelagert,

[4] Geminn, Tatsumi, Terada DÖV 2023, 847 (849).

[5] Geminn, Tatsumi, Terada DÖV 2023, 847 (849).

[6] BMI, OZG-Umsetzungskonzept, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/moderne-verwaltung/ozg-umsetzungskonzept.html, zuletzt abgerufen am 21.02.2024.

[7] Drucksache 20/8093, Entwurf eines Gesetzes zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) https://www.bundestag.de/dokumente/textarchiv/2024/kw08-de-onlinezugangsgesetz-990686, zuletzt abgerufen am 22.02.2024.

[8] Nationaler Normenkontrollrat, Monitor Digitale Verwaltung # 3, Oktober 2019, 3.

[9] BMI, https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-node.html, zuletzt abgerufen am 22.04.2024.

[10] BMI, https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html, zuletzt abgerufen am 22.04.2024.

[11] BMI, https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/efa/efa-node.html, zuletzt abgerufen am 22.04.2024.

[12] Einundfünfzigster Tätigkeitsbericht zum Datenschutz und Fünfter Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, 91 (91-92), https://datenschutz.hessen.de/infothek/taetigkeitsberichte, zuletzt abgerufen am 21.02.2024.

durch die den Onlinedienst betreibende Behörde (Land A) vorgenommen werden oder die ausschließlich aus dem Umstand der elektronischen Bereitstellung der Verwaltungsleistung erwachsen.[13]

Das OZG enthält in seiner aktuellen Fassung keine Antworten auf diese Fragen. Letztlich bedürfte es daher für jede Nachnutzung eines Onlinedienstes nach dem EfA-Prinzip einer individuellen datenschutzrechtlichen Bewertung anhand der Vorschriften der DS-GVO. In praktischer Hinsicht ist hieran problematisch, dass die Digitalisierung von Verwaltungsleistungen nicht homogen einem bestimmten Schema folgt, sondern durch die Gegebenheiten des jeweiligen Digitalisierers (Land A und Dienstleister B) bestimmt ist. In rechtlicher Hinsicht tritt hinzu, dass die Regelungen der DS-GVO ausgelegt werden müssen und zusätzlich das Fachrecht auf die datenschutzrechtliche Bewertung Einfluss nimmt. Durch diese komplexe Gemengelage entstehen Interpretationsspielräume, die in der Praxis zu erheblichen Rechtsunsicherheiten führen. Hinzukommt, dass auch für den Fall, dass die datenschutzrechtlichen Fragen unter Nutzung der von der DS-GVO zur Verfügung gestellten Handlungsinstrumente gelöst werden, allein durch die Anzahl möglicher Akteure und Konstellationen erhebliche Aufwände entstehen (z. B. durch den Abschluss von zahlreichen Auftragsverarbeitungsverträgen nach Art. 28 DS-GVO).

Lösung durch ergänzende datenschutzrechtliche Regelungen im OZG

Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat die datenschutzrechtlichen Herausforderungen der Verwaltungsdigitalisierung bereits frühzeitig erkannt und schon im Herbst 2021 ergänzende gesetzliche Regelungen gefordert.[14] Sie stellte fest, dass die rechtlichen Rahmenbedingungen für eine datenschutzkonforme Umsetzung des EfA-Prinzips im OZG weiterhin nicht geschaffen worden seien und durch den zwangsläufigen Rückgriff auf diverse Übergangsregelungen zur Zuweisung der datenschutzrechtlichen Verantwortlichkeit erhebliche datenschutzrechtliche Risiken und Zweifel an der Rechtmäßigkeit des Verwaltungshandelns entstünden.[15] Um den Gesetzgebungsprozess bezüglich datenschutzrechtlicher Fragestellungen proaktiv zu unterstützen, hat die DSK eine Kontaktgruppe eingesetzt, die die Ausarbeitung des „OZG 2.0“ beratend begleitet hat.[16]

Datenschutzregelungen für Onlinedienste nach dem EfA-Prinzip

Der am 23.02.2024 im Bundestag verabschiedete Entwurf eines Gesetzes zur Änderung des OZG enthält – neben einer Vielzahl weiterer, nicht datenschutzspezifischer Änderungen – in Artikel 1 Nr. 2 und 9 OZG-Änderungsgesetz datenschutzrechtliche Regelungen für Onlinedienste nach dem EfA-Prinzip. Zunächst definiert § 2 Abs. 8 OZG-neu den Begriff des Onlinedienstes. Onlinedienst ist hiernach *„eine IT-Komponente, die ein eigenständiges elektronisches Angebot an die Nutzer darstellt, welches die Abwicklung einer oder mehrerer elektronischer Verwaltungsleistungen von Bund oder Ländern ermöglicht. Der Onlinedienst dient dem elektronischen Ausfüllen der Online-Formulare für Verwaltungsleistungen von Bund oder Ländern, der Offenlegung dieser Daten an die zuständige Fachbehörde sowie der Übermittlung elektronischer Dokumente und Informationen zu Verwaltungsvorgängen an die Nutzer, gegebenenfalls unter Einbindung von Nutzerkonten einschließlich deren Funktion zur Übermittlung von Daten aus einem Nutzerkonto an eine für die Verwaltungsleistung zuständige Behörde. Der Onlinedienst kann auch verfahrensunabhängig und länderübergreifend, insbesondere in der Verantwortung einer Landesbehörde zur Nutzung durch weitere Länder, bereitgestellt werden.“* Sodann normiert § 8a OZG-neu die datenschutzrechtlich relevanten Aspekte der Verwaltungsdigitalisierung nach dem EfA-Prinzip. Nach § 8a Abs. 1 Satz 1 OZG-neu darf die einen Onlinedienst betreibende Behörde (Land A) für die folgenden Zwecke personenbezogene Daten verarbeiten: (1) Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung, (2) Offenlegung der Daten aus dem Online-Formular an die jeweils zuständige Behörde und (3) Übermittlung von elektronischen Dokumenten zu Verwaltungsvorgängen an den Nutzer. Hiervon umfasst sind nach § 8a Abs. 1 Satz 2 OZG-neu auch besondere Kategorien personenbezogener Daten, soweit diese für das angeschlossene Verwaltungsverfahren (Fachverfahren) erforderlich sind. Damit Nutzer die Möglichkeit haben die Bearbeitung eines Online-Formulars zu unterbrechen, schafft § 8a Abs. 2 OZG-neu zudem eine Rechtsgrundlage für die Zwischenspeicherung personenbezogener Daten im Onlinedienst. Ergänzend regelt § 8a Abs. 3 OZG-neu die Modalitäten der Aufbewahrung und Löschung der zwischengespeicherten Daten. § 8a OZG-neu schafft somit Rechtsgrundlagen für die Verarbeitung, um so die im geltenden Recht bestehenden Lücken zu schließen. Die Regelung des § 8a Abs. 4 OZG-neu macht wiederum von der Möglichkeit der gesetzlichen Verantwortungszuweisung

[13] BMI, Eine datenschutzrechtliche Einordnung von Portallösungen und Fachanwendungen in der OZG-Umsetzung, 33 f.

[14] Protokoll der 102. DSK vom 24. und 25 November 2021, Top 10, https://www.datenschutzkonferenz-online.de/protokolle.html, zuletzt abgerufen am 22.02.2024.

[15] Protokoll der 3. Zwischenkonferenz am 21. September 2022, Top 8, https://www.datenschutzkonferenz-online.de/protokolle.html, zuletzt abgerufen am 22.02.2024.

[16] Protokoll der 103. DSK vom 23. bis 24 März 2022, Top 14, https://www.datenschutzkonferenz-online.de/protokolle.html, zuletzt abgerufen am 22.02.2024.

nach Art. 4 Nr. 7 HS 2 DS-GVO Gebrauch. Nach § 8a Abs. 4 Satz 1 OZG-neu liegt die Verantwortlichkeit für die Verarbeitung personenbezogener Daten im Onlinedienst ausschließlich bei der den Onlinedienst betreibenden Behörde (Land A). Hiervon unberührt bleibt nach § 8a Abs. 4 Satz 2 OZG-neu die Verantwortlichkeit der Behörde, an die personenbezogene Daten zum Zwecke der Durchführung des Verwaltungsverfahrens übermittelt werden (Behörde des nachnutzenden Landes/der nachnutzenden Kommune C).

Durch die neu geschaffenen Regelungen entsteht nicht nur für die beteiligten Akteure ein höheres Maß an Rechtssicherheit. Auch für die nutzenden Bürgerinnen und Bürger wird das Handeln der Verwaltung im Kontext der Digitalisierung transparenter und nachvollziehbarer. Weiterhin werden eine Vielzahl andernfalls notwendiger vertraglicher Regelungen (Auftragsverarbeitungsverträge/Vereinbarungen zur gemeinsamen Verantwortlichkeit) durch die gesetzgeberische Verantwortungszuweisung und die neu geschaffenen Rechtsgrundlagen obsolet. Dies dürfte sich positiv auf das Voranschreiten der Verwaltungsdigitalisierung auswirken. Insgesamt sind die datenschutzrechtlichen Regelungen für Onlinedienste nach dem EfA-Prinzip des OZG-neu daher – trotz kleinerer Kritikpunkte – zu begrüßen.[17]

Once-Only-Generalklausel

Sinn und Zweck des Once-Only-Prinzips ist es die Beantragung von digitalen Verwaltungsleistungen einfach, schnell und effektiv zu gestalten. Das Einverständnis der nutzenden Bürgerinnen, Bürger und Unternehmen vorausgesetzt, sollen einmal angegebene Daten wiederverwendet und mit anderen Behörden unkompliziert und sicher ausgetauscht werden können.[18] Hierzu ist es erforderlich, dass die Nutzenden über ein Identifikationsmanagement eindeutig wiedererkannt werden können. An dieser Stelle kommt ein zweites Mammutprojekt der Verwaltungsdigitalisierung zum Tragen: Die Registermodernisierung nach dem Registermodernisierungsgesetz (RegMoG). Das vom RegMoG umfasste Identifikationsnummerngesetzes (IDNrG) legt die Steuer-ID als registerübergreifendes Identifikationsmerkmal fest und ermöglicht hierdurch das Identifikationsmanagement. Denknotwendig geht mit der Schaffung eines einheitlichen, registerübergreifenden Identifikationsmerkmals die Gefahr der Erstellung umfassender Persönlichkeitsprofile einher.[19] Dies wird noch deutlicher, wenn man das Ausmaß der Registermodernisierung betrachtet: Nach Anlage 1 zu § 1 IDNrG werden zunächst 51 Register durch die Steuer-ID als Identifikationsmerkmal miteinander verknüpft. In ihrer Ent-

[17] So bleibt aufgrund des gesetzlichen Wortlauts des § 8 a Abs. 3 Satz 2 OZG-neu beispielsweise unklar, in welchen konkreten Fallkonstellationen eine längerfristige Speicherung der zwischengespeicherten Daten im Onlinedienst zulässig ist.

[18] CIO Bund, https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-verwaltung/registermodernisierung/registermodernisierung-node.html, zuletzt abgerufen am 22.02.2024.

[19] DSK, Entschließung vom 26.08.2020 „Registermodernisierung verfassungskonform umsetzen!", https://www.datenschutzkonferenz-online.de/entschliessungen.html, zuletzt abgerufen am 22.02.2024. Peuker, NVwZ 2021, 1167 (1169).

schließung vom 26. August 2020 „Registermodernisierung verfassungskonform umsetzen!“ hat die DSK auf die hiermit einhergehenden Gefahren für den Persönlichkeitsrechtsschutz hingewiesen. Auch an anderer Stelle wurden Bedenken an der Registermodernisierung geäußert.[20]

Um die mit der Registermodernisierung einhergehenden Risiken zu minimieren, wurden insbesondere in den §§ 2 Nr. 3 und 9 IDNrG Regelungen zum Schutz der Rechte und Freiheiten der Betroffenen aufgenommen. § 2 Nr. 3 IDNrG verpflichtet registerführende Stellen natürlichen Personen die Übermittlung ihrer Daten unter Verwendung der Identifikationsnummer digital über eine zentrale Stelle transparent zu machen (Datenschutzcockpit). Hierdurch soll es Bürgerinnen und Bürgern ermöglicht werden den Überblick über die entstandenen Datenübermittlungen zu behalten.[21] Flankierend ordnet § 9 Abs. 1 IDNrG an, dass Datenübermittlungen zwischen öffentlichen Stellen unter Nutzung einer Identifikationsnummer zu protokollieren sind. Nach § 9 Abs. 2 IDNrG dürfen die Protokolldaten nur zur datenschutzrechtlichen Prüfung sowie zur Gewährleistung der datenschutzrechtlichen Rechte der betroffenen Person, einschließlich der Übermittlung an das Datenschutzcockpit, verwendet werden.

Auch wenn die zuvor dargestellten Entwicklungen rund um das OZG-Änderungsgesetz zu begrüßen sind – mit der Erweiterung der Once-Only-Generalklausel in § 5 E-Government-Gesetz (EGovG-neu) und der hieraus resultierenden Verknüpfung der Regelungen des OZG-neu mit den Regelungen des IDNrG verbleibt aus der Perspektive des Datenschutzes ein Wermutstropfen.

Durch Artikel 2 Nr. 8 des OZG-Änderungsgesetzes soll § 5 Abs. 4 E-EGovG-neu nun folgenden Wortlaut erhalten:

„Soll der Nachweis aus einem Register, welches in der Anlage zum Identifikationsnummerngesetz (...) aufgeführt ist, abgerufen werden, darf die nachweisanfordernde Stelle die Identifikationsnummer nach § 1 des Identifikationsnummerngesetzes zur Zuordnung der Datensätze zum Antragsteller und zum Abruf des Nachweises an die nachweisliefernde Stelle übermitteln. Das Nachweisabrufersuchen darf zusätzlich weitere Daten im Sinne von § 4 Absatz 2 und 3 des Identifikationsnummerngesetzes, in der Regel das Geburtsdatum, zur Validierung der Zuordnung enthalten. Zu diesem Zweck darf die nachweisliefernde Stelle diese Daten verarbeiten.“ Die in § 5 Abs. 4 E-GovG-neu beschriebene Verarbeitung ist nicht von der Regelung des § 2 Nr. 3 IDNrG umfasst, da die Vorschrift nur die registerführenden Behörden, nicht aber diejenigen öffentlichen Stellen, die sich zum Zwecke des Abrufs an sie wenden, adressiert. Findet somit trotz Anfrage seitens der nachweisanfordernden Behörde keine Datenübermittlung durch die Registerbehörde statt, wird dieser Vorgang nicht im Datenschutzcockpit erfasst und bleibt für Bürgerinnen und Bürger somit intransparent. Dies ist bedauerlich, zumal das Transparenzdefizit durch geringfüge Anpassungen des gesetzlichen Wortlauts auszuräumen gewesen wäre.[22]

[20] Peuker, NVwZ 2021, 1167 (1169), Botta, NVwZ 2022, 1247 (1250).

[21] Bundesverwaltungsamt (BVA), https://www.bva.bund.de/DE/Services/Behoerden/Verwaltungsdienstleistungen/Registermodernisierung/Informationen-Buerger/informationen_buerger_node.html#doc970168bodyText2, zuletzt abgerufen am 22.04.2024.

[22] Sinnvoll wäre etwa eine Ergänzung des § 10 OZG oder aber eine Ergänzung von § 5 Abs. 4 EGovG-E-neu, mit der die nachweisanfordernden Stellen verpflichtet werden, natürlichen Personen die Übermittlung im Datenschutzcockpit transparent zu machen.

Zusammenfassend lässt sich festhalten: Auch aus datenschutzrechtlicher Sicht bringt die Digitalisierung der Verwaltung Herausforderungen mit sich. Zu begrüßen ist, dass einige dieser Probleme durch den aktuellen Gesetzesentwurf zur Änderung des OZG gelöst werden und hierdurch zukünftig mehr Rechtssicherheit entsteht. Andererseits lässt der Umstand, dass die DSK bereits seit Herbst 2021 ergänzende datenschutzrechtliche Regelungen zum OZG fordert, erahnen, wie viel zeitliche und personelle Ressourcen in den vergangenen 2,5 Jahren allein zur Beantwortung datenschutzrechtlicher Fragen aufgewendet wurden. Diese wären durch ein zügigeres gesetzgeberisches Handeln vermeidbar gewesen. Nicht nur im Rahmen von Digitalisierungsprojekten, sondern auch am Beispiel der Gesetzgebung zum OZG zeigt sich einmal mehr: Datenschutz sollte frühzeitig mitgedacht und von Beginn an berücksichtigt werden. Denn hier gilt die Lebensweisheit des Dalai Lama: „Jede schwierige Situation, die du jetzt meisterst, bleibt dir in der Zukunft erspart."

Über die Autorin

Katja Horlbeck, LL.M. CIPP/E, CIPM
ist Referatsleiterin beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit und u. a. für die Bereiche Beschäftigtendatenschutz, Verwaltungsmodernisierung und Kommunen zuständig. Der Beitrag gibt die persönliche Auffassung der Autorin wieder.

▶ https://datenschutz.hessen.de/

Anzeige

ANTJE KAISER

DATENSCHUTZ IST LANGWEILIG? MIT YOUNGDATA.DE AUF KEINEN FALL!

Das Jugendportal der Datenschutzaufsichtsbehörden des Bundes und der Länder in Kooperation mit der Datenschutzbeauftragten des Kantons Zürich wurde im vergangenen Jahr komplett neu gestaltet. Im Mai 2023 fand der Relaunch statt. Die neue Website youngdata.de ist an das Nutzungsverhalten Jugendlicher angepasst, insbesondere mit der mobilen Version für den schnellen Zugriff über das Smartphone. Dabei will die Website lebensnahe Themen zum Datenschutz spannend und interessant aufbereiten und wendet sich an Jugendliche im Alter von 13 bis 16 Jahren. Die Website ist nicht nur an die User Experience der Jugendlichen angepasst, sondern auch in Themenauswahl, Ansprache und Texten.

Das Ziel ist es, zum Thema Datenschutz zu sensibilisieren und über den Umgang mit eigenen und fremden personenbezogenen Daten aufzuklären.

Was hat Datenschutz mit Medienkompetenz zu tun?

Nur Wenige wissen, dass die Datenschutzbeauftragten in den Bundesländern auch verschiedene Angebote im Bereich der Medienkompetenz haben. Die Motivation für dieses Engagement ist schnell erklärt. Nach dem Willen des europäischen Gesetzgebers ist die Sensibilisierung und Aufklärung der Bürgerinnen und Bürger über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten eine zentrale Aufgabe. Artikel 57 Abs. 1 lit. b DS-GVO hebt in diesem Zusammenhang ausdrücklich die Notwendigkeit spezifischer Maßnahmen für Kinder hervor. Diese Aufgabe ist ein gemeinsames Anliegen der Datenschutzkonferenz des Bundes und der Länder (DSK). Die Seite youngdata.de stellt zusätzlich eine Übersicht über die speziellen Angebote der einzelnen Bundesländer für Jugendliche und Interessierte bereit.

Die Sensibilisierung zum Umgang mit den eigenen Daten, Persönlichkeitsrechten sowie der Wahrung Rechte anderer ist unerlässlich. Dafür ist es notwendig, dass die Nutzenden die Mechanismen und Funktion unserer digitalen Kultur verstehen und kritisch hinterfragen können. Dies setzt jedoch Wissen voraus, etwa zu den Mechanismen, mit denen weltweit agierende Unternehmen personenbezogenen Daten der Bürgerinnen und Bürger aus- und verwerten. Um sich aktiv und kreativ im Netz bewegen zu können, muss man die Vor- und Nachteile dieser Dienste und Anwendungen kennen. Jugendliche diskutieren und klären in der Regel nicht alle Fragen dieses komplexen Themas in der Schule oder im Elternhaus. Was den Umgang mit den eigenen persönlichen Informationen betrifft, hat zudem jeder Mensch auch eine individuelle Position zur Quantität und Qualität der Daten, die er oder sie von sich preisgeben möchte. Die Datenschutzaufsichtsbehörden können aufklären und dadurch Jugendliche und alle Interessierten unterstützen ihre eigenen Werte in Bezug auf ihre persönlichen Informationen aktiv umzusetzen.

Mit youngdata.de möchten sie ihr Fachwissen weitergeben, so dass Jugendliche selbstbestimmt durch unsere digitale Welt gehen können. Die detaillierten Artikel beinhalten konkrete Tipps zum selbstbestimmten Umgang mit den eigenen Daten. Dazu gehören klassische Themen wie Datensicherheit, Tracking oder Privatsphäre als Ware ebenso wie Informationen zu sozialen Netzwerken, Apps oder Hate Speech. Natürlich werden auch neue Entwicklungen wie KI und ChatGPT so vermittelt, dass Jugendliche verstehen können, welche Rolle ihre Daten und persönlichen Informationen dabei spielen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder tragen mit dem Jugendportal youngdata.de aktiv zur souveränen Teilhabe an der digitalisierten Gesellschaft bei. Damit fördern sie nachhaltig den selbstbestimmten Umgang mit den eigenen Daten – und somit die Grundidee des Datenschutzes.

Entstehung von Youngdata.de:

Youngdata wurde im November 2013 vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI RLP) entwickelt. Die Initiierung durch den

Datenschutzbeauftragten in Rheinland-Pfalz war damals ein Novum, das Projekt wurde begeistert von den Kolleginnen und Kollegen in den Ländern aufgenommen. Aus diesem Grund ist dann die Website www.youngdata.de im Februar 2015 in die gemeinsame Verantwortung aller Datenschutzbeauftragten des Bundes und der Länder sowie in Kooperation mit der Datenschutzbehörde des Kantons Zürich übergegangen.

Ende 2021 wurde im DSK Arbeitskreis „Datenschutz und Medienkompetenz" der Relaunch der Website befürwortet und von der Datenschutzkonferenz des Bundes und Länder (DSK) beschlossen. Anfang 2022 fanden sich engagierte Kolleginnen und Kollegen aus Berlin, Hamburg, Mecklenburg-Vorpommern, Rheinland-Pfalz und vom Bundesbeauftragten, die sich dann innerhalb eines Jahres an die Überarbeitung der Website setzten. Die Projektgruppe hat Workshops durchgeführt und sich live getroffen, es fanden unzählige Videokonferenzen und eine intensive Abstimmung statt. Mit der Auftragsvergabe zum Relaunch der Seite wurde es konkret, und sie nahm Form an. Ab da folgten wöchentliche Treffen mit der Agentur, Texte mussten überarbeitet oder komplett neu geschrieben werden. Das Ziel war der Relaunch im ersten Halbjahr 2023. Am 10. Mai war es dann soweit: Die neue Seite ist online.

Youngdata.de holt den 3. Platz beim Medienpreis TOMMI

Das Jugendportal der unabhängigen Datenschutzbehörden des Bundes und der Länder sowie des Kantons Zürich ist preisgekrönt: Am 3. Dezember 2023 wurde die Webseite youngdata.de mit dem 3. Platz in der Kategorie „Jugendpreis Bildung" des renommierten Kindersoftwarepreises TOMMI ausgezeichnet. In der Begründung der Jugendjury heißt es: „Die Webseite Youngdata gewinnt beim TOMMI den 3. Platz, weil es endlich mal für uns Jugendliche eine gute und verständliche Auswahl an Informationen zum Thema Datenschutz gibt. Zwar haben wir einiges schon vorher gewusst, aber eben vieles auch nicht. Der Aufbau ist sehr gut und vor allem haben wir verstanden, dass es beim Thema Datenschutz um uns als Menschen geht und nicht um Daten. So eine Seite würden wir uns auch für die Schule wünschen, wenn es um Medienkompetenz geht."[1]

Das Urteil der Jugendjury ist ein schönes Lob für die Kolleginnen und Kollegen aus den Aufsichtsbehörden in Berlin, Hamburg, Mecklenburg-Vorpommern, Rheinland-Pfalz und dem Bundesbeauftragten, die den Relaunch umgesetzt haben. Gleichzeitig motiviert es die Youngdata-Redaktionsgruppe der Datenschutzaufsichtsbehörden des Bundes und Länder auch in Zukunft Datenschutzthemen für Jugendliche aufzugreifen und über alle aktuellen Themen zu informieren.

Youngdata.de in der Zukunft

Die Vermittlung von Datenschutzbewusstsein als Teil der Medienkompetenz ist unverzichtbar. Jeden Tag werden weltweit riesige Datenmengen mit Informationen produziert, nicht immer nur von Menschen selbst. Diese erreichen uns über die sozialen Medien, über Suchmaschinen, per E-Mail oder als Push-Nachrichten. Die Entwicklungen gehen einher mit immer neuen Apps, digitalen Endgeräten und Tools. Damit sowohl Informationen kritisch bewertet als auch digitale Medien und Tools genutzt werden können, müssen Medienkompetenz und Datenschutzbewusstsein kontinuierlich aktualisiert werden. Gleichermaßen wichtig ist die Aktualisierung und Weiterentwicklung der Website www.youngdata.de.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder in Kooperation mit dem Kanton Zürich werden auch weiterhin ihr Fachwissen teilen, damit Jugendliche und alle Interessierten es nutzen und sich in unserer digitalen Gesellschaft selbstbestimmt, souverän und verantwortungsbewusst bewegen können. Digitale Kompetenz und Datenschutzbewusstsein sind für jeden Menschen – unabhängig des Alters – in der digitalen Gegenwart unerlässlich.

Hier geht es direkt zu Youngdata:

▶ www.youngdata.de

Über die Autorin

Antje Kaiser
ist Referatsleiterin Presse, Kommunikation und Medienbildung beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV)

[1] https://tommi.kids/magazin/spiele/platz-3-https-youngdata-de-konferenz-der-unabhaengigen-datenschutzbehoerden-des-bundes-und-der-laender-dsk-der-landesbeauftragte-fuer-datenschutz-und-informationsfreiheit-mecklenburg-vorpomme/

FRANK SPAEING

BVD UND DVD FÜHREN DATENSCHUTZ-WIKI GEMEINSAM FORT

Mitarbeit erwünscht…

Seit Juli 2023 bietet der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. gemeinsam mit der Deutschen Vereinigung für Datenschutz e.V. (DVD) dem Datenschutz-Wiki eine neue Heimat. Diese Kooperation wurde vereinbart, nachdem sich die Ruhr-Universität Bochum (RUB) aus dem gemeinsamen Betrieb mit dem BvD verabschieden musste. Die RUB und der BvD hatten das Projekt gemeinsam 2016 von der damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) übernommen.

Wesentliches Motiv für ein weiteres Betreiben der Seite ist die konzentrierte Informationssammlung zu maßgeblichen Gesetzen rund um den Datenschutz, die Seite ist frei von möglichen kommerziellen Interessen von Anbietern. Im Datenschutz-Wiki ist nicht nur die Europa-Ebene mit der DSGVO und die Bundesebene mit dem BDSG zu finden, sondern auch alle Landesdatenschutzgesetze sind dort einsehbar. Zurzeit laufen Gespräche, um zu klären, wie der Wiki-Charakter angesichts beschränkter personeller Kapazitäten wieder aktiviert und (wo nötig inhaltlich) aktualisiert werden kann (seit dem Umzug wird das Datenschutz-Wiki im read-only-Modus betrieben).

Insbesondere die DVD verfügt – obgleich bundesweit im Datenschutz politisch aktiv – als gemeinnütziger Verein nur über ein begrenztes finanzielles Budget. Bürobetrieb, Webseite und vor allem die Vereinszeitschrift Datenschutz Nachrichten (DANA) werden über die Mitgliedsbeiträge, die für natürliche Personen bei zurzeit 105,00 Euro liegen, finanziert. Sogenannte Firmenmitglieder, zu denen auch selbstständige Datenschutzbeauftragte gehören können, zahlen mit 220,00 Euro einen höheren Jahresbeitrag, dafür dürfen sie das DVD-Mitgliedslogo auf der Webseite verwenden und damit der interessierten Kundschaft mitteilen, dass sie sich auch für die bürgerrechtliche Seite der Datenschutz-Entwicklung engagieren.

Denn die politische und bürgerrechtliche Arbeit ist das Hauptbetätigungsfeld der DVD. Am 26. November 1977 gegründet hat sie im Laufe der Jahrzehnte vielfältige Stellungnahmen zu Gesetzentwürfen verfasst und seit 1979 in der DANA die gesamte Entwicklung des Datenschutzes kritisch begleitet. Vor allem die bürgerrechtlichen Interessen werden im Verbund mit anderen Bürgerrechtsorganisationen kontinuierlich verfolgt. So ist die DVD seit den ersten Big-BrotherAwards im Jahr 2000 in deren Jury vertreten und unterstützte unter anderem die Demonstrationen „Freiheit statt Angst“, die Kampagne von Campact gegen das Meldegesetz, die bundesweite Initiative gegen verhaltensbasierte Werbung im Internet und die Aktionen gegen das Client-Side-Scanning (CSS), das auch als Chatkontrolle bekannt ist. Regelmäßig bringt sich die DVD auf europäischer Ebene ein, zum Beispiel durch das Unterzeichnen offener Briefe, die durch das EDRi-Netzwerk lanciert werden.

Weitere inhaltliche Schwerpunkte wie die Gesetzgebungs-Entwicklung in Europa (hier sei besonders an die Sonderhefte zu den roten Linien zur Datenschutz-Grundverordnung aus den Jahren 2015 und 2016 erinnert) oder auch das im vergangenen Jahr in Kraft getretene Hinweisgeber-Schutzgesetz als Umsetzung der europäischen Richtlinie zum Whistleblowing werden jeweils durch DANA-Schwerpunkt-Hefte kritisch beleuchtet.

Vor diesem Hintergrund erschien eine Übernahme des Datenschutz-Wiki durchaus folgerichtig. Heinz Alenfelder, ge-

schäftsführendes Vorstandsmitglied: „Die meisten anderen Quellen zur Datenschutz-Gesetzgebung beziehen sich entweder nur auf einen Teilbereich oder sind mit kommerziellem Werbeinteresse hinterlegt." Mit dem Blick des Kassierers ergänzt er: „Natürlich hoffen wir auch darauf, dass wir mit einem gut gepflegten Datenschutz-Wiki weitere Mitstreiter und Mitstreiterinnen für den Datenschutz aus der bürgerrechtlichen Perspektive gewinnen können."

Über den Autor

Frank Spaeing
ist Vorsitzender der Deutschen Vereinigung für Datenschutz e.V. (DVD)

spaeing@datenschutzverein.de

Ihr Engagement macht den Unterschied:

Die DVD verspricht sich von der Kooperation mit dem BvD eine Reaktivierung des Datenschutz-Wikis in seiner eigentlichen Form und möchte ihre Mitglieder zur aktiven Mitarbeit aufrufen. Aber natürlich sind auch alle Leserinnen und Leser der BvD-News eingeladen sich an dem Datenschutz-Wiki zu beteiligen. Wenn Sie Interesse an der zukünftigen Mitgestaltung des Datenschutz-Wikis haben, melden Sie sich bitte unter:

ds-wiki@datenschutzverein.de

Hier gelangen Sie direkt zum Datenschutz-Wiki

datenschutz-wiki.de

Anzeige

Verwaltungsfokus Datenschutz

Als bewährter **Wegweiser für die Kommunalpraxis** unterstützt Sie der ZILKENS/GOLLAN bei allen typischen Datenschutzfragen im Verwaltungsalltag.

Auf neuestem Stand erläutert werden neben allgemeinen **Rechtsgrundlagen, Betroffenenrechten und Dokumentationspflichten** auch bereichsspezifische Fragen: z.B. der Datenschutz im Sozial- und Aufenthaltsrecht, im Pass- und Melderecht, bei der Ratsarbeit oder im Schul- und Gesundheitswesen.

Online informieren und versandkostenfrei bestellen:
www.ESV.info/21270

Datenschutz in der Kommunalverwaltung
Recht – Technik – Organisation

Herausgegeben von
Dr. Martin Zilkens und **Dr. Lutz Gollan**
6., völlig neu bearbeitete Auflage 2023,
902 Seiten, fester Einband, € 118,–
ISBN 978-3-503-21270-5
eBook: € 107,40, ISBN 978-3-503-21271-2

Erich Schmidt Verlag GmbH & Co. KG
Genthiner Str. 30 G · 10785 Berlin
Tel. (030) 25 00 85-475
Fax (030) 25 00 85-275
ESV@ESVmedien.de · www.ESV.info

ESV ERICH SCHMIDT VERLAG
100 Jahre

MARIYA MIHAYLOVA-VARBANOVA

DREI NOMINIERTE FÜR DIE DAME 2023

Ein Magazin-Text, ein Video und eine crossmediale Datenanalyse haben die Chance auf den Datenschutz Medienpreis (Dame) 2023

Zum siebten Mal versammelte sich Ende Februar die Jury des Datenschutz Medienpreises (DAME), um aus einer Vielzahl von Beiträgen die Nominierten auszuwählen. Der Gewinner wird am 28. Mai auf den BvD-Verbandstagen in Berlin bekannt gegeben.

Nominierter Text-Beitrag:

„Im Spinnennetz“ von Holger Fröhlich

In seinem Artikel für das Wirtschaftsmagazin „brand eins“ widmet sich Autor Holger Fröhlich dem „Schattenmarkt der Online-Werbung“ und den Praktiken der AdTech-Unternehmen. Er kommt zu dem Schluss, dass sich die Branche eine nie da gewesene automatisierte Verfolgung und Auswertung von Verhalten im Netzt erlaubt. Daran werde sich auch bald trotz EU-Initiativen nichts ändern, zeigte sich Fröhlich überzeugt. Und das, obwohl sich die meisten Menschen aus einer Sicht sich bewusst sind, wie raffiniert der Handel mit unseren Daten mittlerweile geworden ist.

Jury-Mitglied Frederick Richter zu der Nominierung:

„Wenn ein Artikel sperrige Begriffe wie "Real-Time-Bidding" oder "Demand Side Platform" nicht nur verständlich erklärt, sondern auch die dazugehörigen Zusammenhänge spannend beschreibt, dann ist das schon preisverdächtig. Der Beitrag nimmt die Lesenden mit durch die interessante Geschichte der personalisierten Werbung - und er zeigt auf, dass es auch im digitalen Raum durchaus Werbeformen gibt, die die Privatsphäre weniger beeinträchtigen."

Nominierter Jugend-Beitrag (Video):

„Enkeltrick 2.0-Betrug mit KI“

Betrüger:innen geben sich als Familienmitglieder in einer Notlage aus und fordern von ihren Opfern Geld. Durch die Verwendung öffentlich zugänglicher Daten und die zunehmende Nutzung von KI oder intelligenten Software-Tools, die Stimmen täuschend echt reproduzieren können, wirken diese Betrugsversuche besonders überzeugend.

Wie einfach eine Stimme nachahmbar ist, wie gefährlich der neue Enkeltrick für die potenziellen Opfer sein kann und wie man sich und seine Angehörige davor schützt, zeigen Helene Reiner, Lenja Hülsmann, Marco Lehner und Bianca Taube aus der News-WG von Puls, dem Jugendnetzwerk des Bayerischen Rundfunks in ihrem Instagram-Video.

Screenshot aus dem Instagram-Beitrag

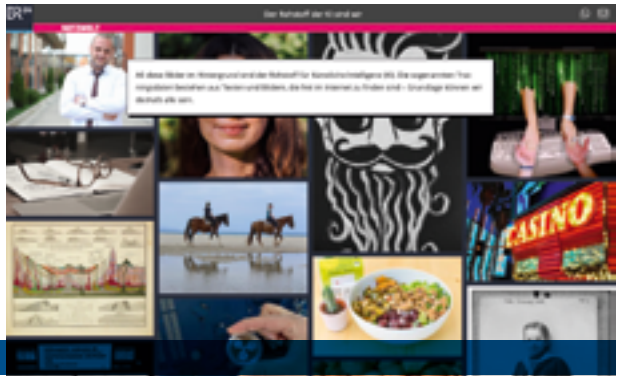
Jury-Mitglied Eric Hohenadel zu der Nominierung:

„Der bemerkenswerte Social Media Beitrag zeigt, wie mithilfe von künstlicher Intelligenz Identitätsdiebstahl verübt werden kann. Mit einem anschaulichen Selbstversuch wird der Appell an Jugendliche gerichtet, die eigenen Daten besser zu schützen und vielleicht auch die ältere Generation über mögliche Gefahren aufzuklären.“

Nominierter Crossmedialer Beitrag:

„Der Rohstoff der KI sind wir“ von Katharina Brunner und Elisa Harlan

Katharina Brunner und Elisa Harlan gehen in ihrer Datenanalyse für den Bayerischen Rundfunk (BR) der Frage nach, wie Crawler Bilder und Texte aus Millionen von Websites als Trainingsdaten für KI-Systeme sammeln. Ein Team aus Datenjournalistinnen hat dafür den größten öffentlich zugänglichen KI-Trainingsdatensatz untersucht, der Grundlage für Bildgeneratoren wie Stable Diffusion ist. Er besteht aus mehr als 5,8 Milliarden Verweisen auf Bilder und ihre Beschreibungen aus dem Internet. Die Vorarbeit dafür leistete das offene Netzwerk LAION. Die Abkürzung steht für Large Scale Artificial Intelligence Open Network und ist ein Zusammenschluss von Freiwilligen überwiegend aus Europa und Nordamerika. Die britische Firma Stability AI zahlte für LAION und eine Forschungsgruppe der Ludwig-Maximilians-Universität München die notwendige Rechenleistung.



Screenshot aus dem Beitrag "Der Rohstoff der KI sind wir."

Das Ergebnis der Recherche: Die Daten enthalten viele sensible und private Informationen wie Nacktfotos, Bankdaten und genaue Angaben, wo ein Foto aufgenommen wurde. Viele Betroffene sind sich dessen nicht bewusst, befanden die Autorinnen. Und sie zeigen, wie die KI-Unternehmen auf Anfragen nach Löschung privater Bilder auf Basis der DSGVO reagieren.

Jury-Mitglied Tobias Meisel zu der Nominierung:

„Der Rohstoff der KI sind wir" beleuchtet eindrucksvoll die Rolle persönlicher Daten in der KI-Entwicklung und betont die Notwendigkeit ethischer Standards in der KI-Forschung. Mit seiner ansprechenden Aufmachung, die interaktive Elemente und visuell ansprechende Grafiken nutzt, gelingt es den Autorinnen hervorragend, komplexe Inhalte fesselnd und verständlich zu präsentieren. Dies macht den Beitrag zu einem potenziellen Gewinner."

Die Jury des Datenschutz Medienpreises 2023:

Stefanie Rack Päd. Referentin klicksafe, Medienanstalt Rheinland-Pfalz

Eric Hohenadel klicksafe-Jugendjuror

Frederick Richter Vorstand Stiftung Datenschutz

Lars Kolan Geschäftsstellenleiter Deutscher Spendenrat

Dr. Christoph Bausewein Vorstandsmitglied des BvD und Geschäftsführer von privacy4people

Tobias Meisel Referent der DATEV-Stiftung Zukunft

Barbara Thiel Landesbeauftragte für den Datenschutz Niedersachsen a. D.

Marion Zinkeler Vorständin Verbraucherzentrale Bayern

Weitere Informationen finden Sie unter:

▶ https://www.bvdnet.de/datenschutzmedienpreis/

Die drei nominierten Beiträge finden Sie auf

▶ www.datenschutzmedienpreis.de

Über die Autorin

Mariya Mihaylova-Varbanova

ist Mitarbeiterin in der Geschäftsstelle des BvD und zuständig für den Datenschutz Medienpreis DAME. Zugleich betreut sie die Initiative Datenschutz geht zur Schule der Privacy 4 People gGmbH.

Medienpartner: klicksafe

Förderer: DATEVSTIFTUNG ZUKUNFT, STIFTUNG DATENSCHUTZ, Deutscher Spendenrat e.V. Die gute Tat im Blick

DOZENT:INNEN-TAG DSGZS

Das Dozent:innentreffen der Initiative „Datenschutz geht zur Schule“ (DSgzS) stand ganz im Zeichen des Themas Künstliche Intelligenz

Erfurt (BvD). Ende November 2023 hatte die Initiative „Datenschutz geht zur Schule“ (DSgzS) ihre Aktiven nach Erfurt ins evangelische Augustinerkloster eingeladen. In dessen moderner Bibliothek erlebten die Teilnehmenden mehrere Vorträge, die sich fast alle mit dem Thema Künstliche Intelligenz beschäftigten.

Nachdem Rudi Kramer als Sprecher des AK Schule den Dozent:innentag eröffnet hatte, startete das Programm mit einem Vortrag von René Rösel über Digitalisierung in der Schule. Rösel sprach stellvertretend für Thüringens Landesdatenschutzbeauftragten (TLfDI) Lutz Hasse, der kurzfristig verhindert war. Die Infos wurden besonders verständlich durch eine klare Aufteilung der Themen in die Kategorien Problem, Ursache, Lösung und Wer macht's? Von allgemeinen Problemstellungen ging es schnell zum Überthema KI und dessen datenschutzrechtlichen Herausforderungen.

Es folgte Stephan Jauch vom TLfDI, der in seinem Vortrag „Künstliche Intelligenz vs. Mensch?“ grundlegend in das Thema KI einführte. Ein Schwerpunkt lag dabei auf der Frage, wie sich die Arbeitswelt durch KI verändern wird.

Frederick Richter von der Stiftung Datenschutz präsentierte den Status quo bei der komplexen Diskussion, ab wann Daten als anonymisiert oder zumindest pseudonymisiert einzustufen sind. Sehr verständlich wurde die aktuelle Rechtsprechung des EuGH hierzu vorgestellt. Dazu hat die Stiftung Datenschutz einen Praxisleitfaden veröffentlicht.

Der Professor für Digitale Forensik von der Hochschule Mittweida, Dirk Labudde, müsste eigentlich einen Preis für den unterhaltsamsten Vortrag erhalten. Dabei war sein Thema Cyberkriminalität wenig lustig: Es ging unter anderem um Identitätsdiebstahl, Social Engineering, Deep Fakes, Grooming und den Einsatz von KI als Werkzeug von Kriminellen.

Jan Rozek von der Bahn-Tochter DB Systel erläuterte, wie ein Großkonzern über stringentes Informationssicherheitsmanagement einer Vielzahl von Vorfällen und Meldungen begegnet und diese dokumentiert.

Zum Abschluss stellte David Heimburger, stellvertretender Sprecher des AK Schule, das neue Konzept für die zukünftige Arbeit von DSgzS vor. Die Initiative plant, einen überarbeiteten Foliensatz unter einer Creative-Commons-Lizenz zu veröffentlichen, so dass jede:r Interessierte ohne vorheriges Freigabeverfahren an Schulen Vorträge zum Datenschutz halten kann – inklusive Informationen zu den Chancen und Risiken von KI.

Dozent:innen-Ausflug zum KiKa

Bereits am Vortag hatten acht der DsgzS-Dozent:innen in der Erfurter Jenaplanschule Kinder und Jugendliche für Datenschutz sensibilisiert. Anschließend besuchten die Teilnehmenden des Dozent:innen-Treffens den beim MDR ansässigen Kinderkanal KiKa von ARD und ZDF.

Datenschutz geht zur Schule ist ein Projekt der Privacy 4 People gGmbH. Sie verfolgt Bildungs- und Erziehungszwecke und unterstützt die Förderung von Wissenschaft und Forschung und die Stärkung des Verbraucherschutzes. *dh*

LINK-TIPP

Empfehlungen zum Datenschutz für kleine und mittlere Betriebe finden Sie unter anderem hier:

Werkzeugkasten für den Betrieb der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

▶ https://www.ldi.nrw.de/kmu

Informationen für kleine und mittlere Betriebe des Landesbeauftragten für den Datenschutz Sachsen-Anhalt

▶ https://datenschutz.sachsen-anhalt.de/informationen/infopakete/infopaket-kmu/

Datenschutz für Kleinunternehmen der Stiftung Datenschutz

▶ https://ds-kleinunternehmen.de/startseite

Welche Homepage und/oder Link können Sie empfehlen? Schreiben Sie uns an bvd-news@bvdnet.de.

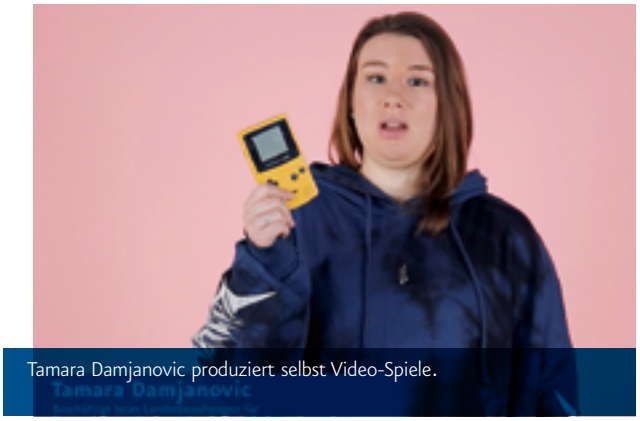
NEUE VIDEOS FÜR DSGZS

Dr. Tobias O. Keber, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-WürttembergTamara Damjanovic

Berlin (BvD). Datenschutz für Schülerinnen und Schüler „leicht erklärt" – dass ist die Idee der Erklär-Videos, die die Initiative „Datenschutz geht zur Schule" (DSgzS) in Kooperation mit den Datenschutzaufsichtsbehörden aus Bayern, Baden-Württemberg, Hessen und Thüringen produzierte. Anlässlich des Safer Internet Days am 6. Februar, brachte DSgzS nun sechs weitere zwei- bis vierminütige Clips heraus. Darin erklären Fachleute leicht verständlich, warum es wichtig ist personenbezogene Daten zu schützen und wie dies ganz praktisch an Laptop, Pad und Smartphone funktioniert.

Themen der neuen Clips sind unter anderem Gaming, Cookies und das Thema Informationsfreiheit. Insgesamt liegen nun 25 Clips vor, die sich jeweils einem speziellen Augenmerk des Datenschutzes für Jugendliche widmen.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Prof. Dr. Tobias Keber, hob zur Vorstellung der neuen Clips hervor, dass die Datenschutz-Grundverordnung Kinder und Jugendliche besonders schütze. Von daher lieferten die Clips wertvolle Datenschutzhinweise auch für Eltern und Lehrkräfte.



Tamara Damjanovic produziert selbst Video-Spiele.

Die bundesweite Initiative DSgzS wird von der gemeinnützigen Privacy4People gGmbH des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. getragen. Unterstützt wird die gemeinnützige Initiative durch die DATEV Stiftung Zukunft.

Es wird immer wichtiger, dass Kinder und Jugendlichen sich bewusst sind, welche Stellschrauben im Umgang mit den eigenen Daten oder den Daten anderer sie selbst nutzen können, um hier eigenverantwortlich zu agieren, betont Rudi Kramer, Sprecher der ehrenamtlichen Initiative des BvD.

chd

Schülerin Sofia erklärt, wie Jugendliche an amtliche Informationen kommen

Hier kommen Sie direkt zu den Videoclips:

▶ https://www.datenschutz-leicht-erklaert.de

Mehr über DSgzS finden Sie hier:

▶ https://www.bvdnet.de/datenschutz-geht-zur-schule/; https://www.dsgzs.de

DATENSCHUTZ-SANKTIONENRECHT

HANDBUCH FÜR DIE UNTERNEHMENS- UND ANWALTSPRAXIS

Dr. Arne Klaas, Prof. Dr. Carsten Momsen, Tim Wybitul

Der Schwerpunkt des Handbuchs liegt auf der Ahndung von Verstößen gegen das materielle Datenschutzrecht, konzentriert sich also auf die hoheitlichen Sanktionen, und beleuchtet die zunehmende Bedeutung des Datenschutzsanktionenrechts. Das Recht ist bisher noch wenig erforscht und viele praktische Fragen sind noch ungeklärt – nicht zuletzt aufgrund der Wechselwirkung zwischen unionsrechtlichen Vorgaben und nationalen Regelungen, die Interpretationsfragen und Kompetenzkonflikte aufwerfen.

Die Herausgeber und Autoren dieses Handbuchs sind angesehene Experten sowohl in der Wissenschaft als auch in der Praxis des Datenschutz-, Straf- und Bußgeldrechts. Dies sorgt für eine ausgewogene Perspektive zwischen Wissenschaftlern und Akteuren der Sanktionspraxis. Hinzu kommt, dass bei strittigen Rechtsfragen Behördenvertreter das Auslegungsergebnis in Frage stellen. Dem Verständnis dient, dass dies unmittelbar in den entsprechenden Kapiteln erfolgt. Hilfreich und informativ sind außerdem die hervorgehobenen Praxistipps. An der einen oder anderen Stelle veranschaulichen Grafiken das Zahlenmaterial.

Nahezu jedes Hauptkapitel beginnt mit einem Überblick oder einer kurzen Einleitung, was dem Leser einen Einstieg in das jeweilige Thema ermöglicht und die Orientierung innerhalb des Buches erleichtert.

Das Handbuch richtet sich an Unternehmen und Datenschutzexperten und vermittelt, wie sie angemessen mit Bußgeldern und Abschöpfungen und den damit verbundenen Herausforderungen umgehen können. Es ist gleichermaßen nützlich für Anwälte, die präventiv beraten, Strafverteidiger, Unternehmensjuristen sowie betriebliche und behördliche Datenschutzbeauftragte. Besonders wertvoll sind die zahlreichen und detaillierten Einblicke in die Bußgeldpraxis der Datenschutzaufsichtsbehörden.

Dr. Arne Klaas, Prof. Dr. Carsten Momsen, Tim Wybitul
DATENSCHUTZSANKTIONENRECHT
Handbuch für die Unternehmens- und Anwaltspraxis

C.H.Beck

5. Auflage 2023
552 Seiten
159,00 Euro (brutto)
ISBN: 978-3-406-79459-9

Der Beck-Verlag bietet auf seiner Webseite das Inhaltsverzeichnis zur Einsicht an https://cdn-assetservice.ecom-api.beck-shop.de/product/inhaltsverzeichnis/34059174/inhaltsverzeichnis-klaas-momsen-wybitul-datenschutzsanktionenrecht-9783406794599.pdf.

Das Buch gliedert sich sieben Teile:

1. Teil: Das Datenschutzsanktionenrecht (Einleitung – auch auf der Beck-Seite abrufbar).
2. Teil: Materielles Recht
3. Teil: Die Verfolgung von bußgeldbewehrten Datenschutzverstößen
4. Teil: Materielles Strafrecht
5. Teil: Die Verfolgung von Datenschutzstraftaten
6. Teil: Gemeinsame Aspekte von Bußgeldern und Straftatbeständen
7. Teil: Datenschutzsanktionenrecht in den USA

Das Sachverzeichnis erscheint mir etwas kurz, während das Inhaltsverzeichnis äußerst detailliert und strukturiert ist,

was die Navigation im Buch erleichtert. Das Quellen- und Literaturverzeichnis ist beeindruckend umfangreich.

Das Handbuch gibt auch betrieblichen und behördlichen Datenschutzbeauftragten zuverlässige Ratschläge im Umgang mit Geldbußen gemäß der DSGVO und den strafrechtlichen Konsequenzen bei Datenschutzverstößen. Es liefert verständliche Antworten und praktische Unterstützung für Datenschutzpraktiker.

Zu den behandelten Themen gehören unter anderem:

- Verständliche Erläuterung der Voraussetzungen für Bußgelder und strafrechtliche Haftung
- Maßnahmen zur präventiven Haftungsvermeidung durch effektive Datenschutz-Compliance
- Richtiges Vorgehen bei Datenschutzvorfällen
- Prozessuale und taktische Überlegungen im Zusammenhang mit Ermittlungsverfahren bei Datenschutzverstößen
- Konflikte zwischen Datenschutzmeldung, Kooperation und Haftung sowie dem Recht sich nicht selbst belasten zu müssen

Um eine ausgewogene Sichtweise zu bieten, kommen verschiedene Akteure aus der Sanktionspraxis zu Wort. Sie gewähren interessante Einblicke in die Sanktionspraxis ihrer Organisationen, geben Empfehlungen zur Gewichtung bei der Verhängung von Sanktionen und zeigen auf, wie eine kooperative Beziehung zu Behörden sanktionsmildernd gestaltet werden kann.

Ein innovatives Element des Handbuchs ist die Möglichkeit für Behördenvertreter und Rechtsanwälte unterschiedliche rechtliche Standpunkte kritisch zu hinterfragen und darzulegen.

Gegensätzliche Auffassungen und ihre Argumente werden im Zusammenhang mit den jeweiligen Rechtsfragen herausgearbeitet. Zusätzlich bietet das Buch konkrete Praxisbeispiele der Autoren, um den praxisorientierten Ansatz zu vertiefen.

Last but not least sei noch kurz auf das siebte und letzte Kapitel hingewiesen, das sich mit dem Datenschutzsanktionenrecht in den USA befasst und erhebliche Unterschiede zum europäischen Rechtsrahmen aufweist. In § 33 wird ein kurzer, aber übersichtlicher Überblick über die datenschutzrechtlichen Vorgaben der US-amerikanischen Bundesgesetze gegeben.

Fazit:

Abschließend kann gesagt werden, dass dieses Buch im Umgang mit Sanktionen wegen Datenschutzverstößen das erste umfassende Praxishandbuch seiner Art ist. Es zeichnet sich durch seine verständliche und gleichzeitig wissenschaftlich fundierte Herangehensweise aus. Die Verknüpfung der verschiedenen Sichtweisen mit rechtlichen Fragestellungen und taktischen Strategien macht, neben den Praxistipps, dieses Buch äußerst wertvoll für Datenschutzexperten, Rechtsanwälte und alle, die mit komplexen Datenschutzfragen zu tun haben.

Prädikat: Sehr empfehlenswert.

Rezension von

Regina Mühlich (CIPM)
ist Wirtschaftsjuristin und Geschäftsführerin der AdOrga Solutions GmbH. Sie ist als externe Datenschutzbeauftragte und -auditorin, Informationssicherheitsbeauftragte sowie Compliance Officer tätig.

▶ AdOrgaSolutions.de

DSGVO/GDSG-KOMMENTAR

DATENSCHUTZ-GRUNDVERORDNUNG, BUNDES-DATENSCHUTZGESETZ UND NEBENGESETZE

Martin Eßer, Philipp Kramer, Kai von Lewinski (Hrsg.) (Auernhammer)

Der „Auernhammer" ist ein Standardwerk zur Kommentierung datenschutzrechtlicher Vorschriften, das bereits zu den Urzeiten des BDSG zur Unterstützung der Umsetzung gesetzlicher Datenschutzvorgaben herangezogen wurde. Mittlerweile wird der ursprüngliche Herausgeber nur noch in Klammern genannt, denn die Prägung durch die neuen Herausgeber, die das Werk bereits seit der 4. Auflage betreuen, ist doch zu dominant geworden. Sie vereinen in diesem Kommentar nicht nur die Kommentierung zur DS-GVO und zum BDSG, auch das TTDSG wird ausführlich kommentiert. Ebenso ist eine Einführung zur Richtlinie 2016/680 (Polizei und Justiz), aber auch eine auszugsweise Kommentierung aus dem Informationsfreiheitsgesetz enthalten.

Mit einer guten Mischung der Autorinnen und Autoren aus Wissenschaft und Praxis, die sowohl beratende Expertinnen und Experte aus Kanzleien wie auch aus Aufsichtsbehörden umfasst, wird die Praxisnähe wie auch Berücksichtigung der Interpretation durch Aufsichtsbehörden gewährleistet.

Die jeweiligen diskussionswürdigen aktuellen Fragestellungen wie z.B. zur Anonymisierung von personenbezogenen Daten (im Kommentar bei Art. 4 thematisiert), die Folgen des EuGH-Urteils C311/18 (Schrems II) bei den an Forderungen an Garantien im Drittstaatentransfer oder auch der Umgang mit § 26 BDSG nach dem EuGH-Urteil (C-34/21) finden sich nachvollziehbar und gut abgebildet. Gleiches gilt für die verschiedenen Fragestellungen im TTDSG wie zum „Zugriff" und zur Gestaltung der Einwilligungsabfrage, die bei § 25 TTDSG diskutiert werden.

Die Zusammenführung der im Alltag wichtigsten Regelwerke in einem Kommentar hilft schnell und zuverlässig mit einer guten und praxisnahen Darstellung eine zitierfähige Quelle für die Begründung von Entscheidungen zu finden. Allein die Form des gewählten Mediums ohne die Möglichkeit eines Onlinezugriffs auf Aktualisierungen wirkt sich angesichts der derzeitig rasanten Rechtsprechung des EuGH und der gesetzgeberischen Aktivitäten nachteilig aus. Trotzdem bleibt es ein empfehlenswertes Werk, das kompakt die relevanten Fragestellungen erschließt.

Martin Esser, Philipp Kramer, Kai von Lewinski (Hrsg.) (Auernhammer)

DSGVO/BDSG
Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und Nebengesetze. Kommentar

Carl Heymanns Verlag

8. Auflage, 2024
3.000 Seiten
159,00 Euro
ISBN-13: 978-3-452-30030-0

Rezension von

Rudi Kramer
ist Syndikusanwalt und Sprecher der AK Schule sowie des AK Finanzdienstleistungen im BvD e.V.

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE

Die wichtigsten Daten der BvD-Gremien

Detaillierte Informationen zu den Treffen und Terminen finden Sie unter:

- bvdnet.de/regionalgruppen
- bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

26.04.2024	RG Schwäbisch Gmünd	**06.06.2024**	RG Nord
06.05.2024	RG Schwäbisch Gmünd	**07.06.2024**	RG Ulm
14.05.2024	RG Ost	**14.06.2024**	RG Karlsruhe
16.05.2024	RG Gütersloh	**21.06.2024**	RG Stuttgart
03.06.2024	RG Schwäbisch Gmünd	**01.07.2024**	RG Schwäbisch Gmünd

Sie möchten zu einem Thema aktiv mitmachen oder in Erfahrungsaustausch mit Kollegen treten?

Termine und Anmeldung finden Sie auf unserer Webseite:

- bvdnet.de/termine/

BVD-STELLENBÖRSE

Sie suchen ausgewiesenes Datenschutz-Knowhow für Ihr Unternehmen? Mit einer Anzeige in der BvD-Stellenbörse finden Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:

- bvdnet.de/bvd-stellenboerse

VERNETZEN SIE SICH MIT UNS:

- bvdnet.de

Mastodon: mastodon.social/@bvd@privacyofficers.social

LinkedIn: linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BLOG: bvdnet.de/themen/bvd-blog/

RSS-Feed: bvdnet.de/feed/

BVD PARTNERSHIP PROGRAM

Mit seinem Partnership Program bietet der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. Unternehmen die Möglichkeit die Sichtbarkeit in ihrer Zielgruppe zu erhöhen und somit ihre Marke vor einer der größten Gemeinschaften von Datenschutzfachleuten in Deutschland zu präsentieren. Bei BvD-Events können die Partner zudem vom BvD-Netzwerk profitieren und wertvolle Kontakte knüpfen.

Gleichzeitig tragen Partner durch ihr finanzielles Engagement dazu bei die Beiträge für die BvD-Mitglieder stabil zu halten. Dem Verband wird außerdem ermöglicht seine von den Satzungszwecken vorgegeben Aktivitäten weiter auszubauen. Denn die zunehmende Komplexität unserer Kommunikationsgesellschaft erfordert einen starken Berufsverband für Datenschutzbeauftragte.

Bei der Auswahl geeigneter Partner hat sich der BvD auf einen Code of Conduct verpflichtet, welcher die Integrität, Neutralität und die Wahrung der Verbandssatzung sicherstellt.

» Bei Fragen zu oder Interesse an einer Partnerschaft wenden Sie sich bitte an:

Karsten Füllhaase
Geschäftsführer
Tel. +49 (0)30 20 62 14 41

▶ karsten.fuellhaase@bvdnet.de

Wir danken unseren Silver Partnern:

caralegal

▶ caralegal.eu

WEITERE WICHTIGE KONTAKTE

An dieser Stelle informiert Sie der BvD über aktuelle Kontakte zu Personen, Institutionen und Anbietern sowie wichtigen Partnern. Gerne können Sie sich hier mit Ihrem Angebot, Ihren Dienstleistungen und Ihrem Portfolio präsentieren.

Informationen zu Anzeigen und Werbemöglichkeiten in der BvD-News erhalten Sie unter bvd-news@bvdnet.de.

Marketing

FÜR DEN BESTEN
EINDRUCK
www.tpdigitaldruck.de
Trend Point Marketing GmbH
Breitenbachstraße 24-29 | 13509 Berlin

Wettbewerb

Datenschutz Medienpreis 2023
Die Preisverleihung erfolgt am 28. Mai 2024 auf den BvD-Verbandstagen in Berlin.
DAME 2023

Schulprojekt

"Datenschutz geht zur Schule" – DSgzS
Ein Projekt der Privacy4People gGmbH
Budapester Straße 31 · 10787 Berlin
Telefon (030) 26 36 77 58 · Telefax (030) 26 36 77 63
dsgzs@dsgzs.de · www.dsgzs.de

privacy4people
privacy4people - Gesellschaft zur Förderung des Datenschutzes gGmbH
IHRE SPENDE FÜR DEN DATENSCHUTZ:
Commerzbank
IBAN: DE 30 5054 0028 0424 5577 00
BIC: COBADEFFXXX
Telefon: +49 30 20 62 14 41
mail@privacy4people.de • privacy4people.de

Anzeige

DSGVO-GUARD®

AUTOMATISIERTE WEBSITE- UND SHOP-AUDITS.

INKL. DATENSCHUTZERKLÄRUNG UND CO. PER MAUSKLICK.

DIE LÖSUNG FÜR PRIVACY PROFESSIONALS

- Zugriff auf eine riesige von Fachanwälten geführte Datenbank für Webdienste und Cookies
- KI-gestützte Datenstromanalyse von Websites mit rechtlicher Qualifizierung von Webdiensten, Cookies und Co.
- Rechtstexte als White-Label für Websites und Onlineshops: Datenschutzerklärung, Impressum, AGB, etc.

Website-Audits inkl. Rechtstexten

Jetzt kostenfreie Lizenz sichern!

>> https://website-check.de/dsgvo-guard <<

Automatisierte Echtzeit-Lösung.

Der DSGVO-GUARD® ist ein Service der Website-Check GmbH - Beethovenstrasse 24, 66111 Saarbrücken

Anzeige

decareto

Capterra 4.8

der DSGVO Scanner mit den zufriedensten Kunden

*auf capterra.com.de

Überzeugen Sie sich selbst & sichern Sie sich noch heute exklusiven Rabatt!

decareto.de/bvd

★★★★★
„Unverzichtbares Tool“

★★★★★
„Beste Hilfe im Dschungel der Website Tools“

★★★★★
„Die Webseiten-Tests unterstützen mich bei der Betreuung meiner Datenschutzkunden optimal.“

★★★★★
„Die Wunderwaffe bei der datenschutzrechtlichen Bewertung von Websites“

★★★★★
„Ich kann keinen Punkt finden, den ich an decareto nicht mag.“

★★★★★
„Bestes Scantool für Webseiten auf DSGVO-Konformität“

★★★★★
„Die Prüfung von Webseiten auf datenschutzrechtliche Schwachstellen war noch nie so einfach“

★★★★☆
„Die Bedienung dieses Tools ist sehr einfach und spart uns im Arbeitsalltag viel Zeit!“

★★★★★
„Gelungene, praxisorientierte Software und ein sehr guter Service!“