Ausgabe 02/2023

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Seite 6

EINE NEUE EPOCHE? DIE BVD-VERBANDSTAGE DISKUTIERTEN ÜBER CYBERCRIME UND KI

Christina Denz, Jürgen Hartz

Seite 10

KENNZEICHNUNGS-PFLICHTEN FÜR KI AUS PERSPEKTIVE DER ETHIK

Jessica Heesen

Seite 18

„WIR MÜSSEN IN EINE ART DURCHSETZUNGS-KULTUR SWITCHEN“

Interview mit Max Schrems

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

mastodon.social/@bvd@privacyofficers.social

linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD e.V.
DATENSCHUTZ GESTALTEN

Alle Infos: **www.bvdnet.de/herbstkonferenz-datenschutz**

Treffpunkt der Datenschutz-Community – jetzt anmelden!

BvD-Herbstkonferenz & Behördentag

18.10. – 20.10.2023

Im NH München Ost Conference Center

Next Level Privacy:

Fit für die Zukunft

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Mit spannenden Keynotes:

- **Digital- und Datenrecht 2025**
  Prof. Dr. Tobias Keber, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg
- **European Mobility Data Space (KI im Fahrzeug, wem gehören die Daten)**
  Benjamin Brake, Bundesministerium für Digitales und Verkehr
- **Ausgespäht und abkassiert? Nein danke!**
  Erik Manke, Polizei Hamburg sowie Fachbereichsvertreter Kriminalpolizei der Gewerkschaft der Polizei
- **Herausforderung KI: Datenschutz als Königsdiziplin im Dekathlon der Grundrechte?**
  Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein

Jetzt anmelden:

Gemeinsame Konferenz von:

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg

BayLDA

BvD e.V. DATENSCHUTZ GESTALTEN

Liebe Leserinnen und Leser,

„Können wir uns Datenschutz noch leisten?" lautete etwas provokativ das Motto der BvD-Verbandstage, die im Mai mit Rekordbeteiligung in Berlin stattfanden. Die Antwort auf diese Frage lautet natürlich: Wir können nicht nur, wir müssen uns Datenschutz leisten. Doch wie wir alle wissen, gibt es auch Stimmen aus der Politik, die hartnäckig argumentieren, dass wir im Interesse des Fortschritts und der Innovation Datenschutzkompromisse eingehen sollten. Oder es werden gar andere schützenswerte Güter wie die Gesundheit gegen das Recht auf informationelle Selbstbestimmung ausgespielt. Tatsächlich ist es alles andere als innovativ, Bürgerrechte bei der Entwicklung neuer digitaler Lösungen außen vor zu lassen – insbesondere deshalb, weil die DSGVO zum Vorbild für neue Datenschutzgesetze weltweit geworden ist. Trotzdem sind wir gut beraten, uns mit diesen Positionen auseinanderzusetzen, um sie effizient widerlegen zu können.

Dabei macht es sich der BvD zur Aufgabe, den Datenschutz nicht nur als ethisches oder moralisches Gebot oder als rechtliche Verpflichtung ins Bewusstsein zu rücken, sondern vor allem auch als Chance. Eine Chance für Unternehmen, das Vertrauen ihrer Kunden zu gewinnen, ihre Wettbewerbsfähigkeit zu steigern und durch ein gesteigertes Bewusstsein für Datenschutz auch die stetig wachsende Bedeutung von Datensicherheit zu erkennen und entsprechend zu handeln. Eine Chance für Deutschland und Europa, unsere Werte und Grundrechte zu verteidigen und unsere digitale Souveränität zu sichern. Und eine Chance für jeden Einzelnen von uns, die Kontrolle über unsere eigenen Daten zu behalten und unser digitales Leben in Einklang mit unseren Werten und Bedürfnissen zu gestalten.

Allerdings ist es keine lapidare Aufgabe, diese Chancen zu nutzen. Für uns Datenschutzbeauftragte bedeuten wachsende Komplexität sowohl auf der technischen als auch auf der juristischen Seite: Die Anforderungen an unsere Beratung werden stets umfangreicher, und es gilt am Ball zu bleiben, um Verantwortliche bei einer praktikablen Umsetzung datenschutzkonformer Geschäftsprozesse kompetent zu begleiten.

Unsere BvD-News möchten Sie dabei unterstützen, indem wir Sie über aktuelle Entwicklungen auf dem Laufenden halten. Ein Aspekt, der dabei immer mehr an Bedeutung gewinnt, ist das Thema Cybersicherheit, dem gleich zwei ausführlichere Artikel in dieser Ausgabe gewidmet sind. In aller Munde ist derzeit auch das Thema generative KI. Zudem berichten wir über die Initiative der Aufsichtsbehörden zu ChatGPT, ein Verfahren für eine KI-Kennzeichnung und den aktuellen Stand der Debatte bei Gesundheitsdaten und elektronischer Patientenakte. Weitere Themen sind beispielsweise die Bestandsdatenauskunft nach TTDSG, das Strafrecht beim Datenschutz und bei DSB, der „Dauerbrenner" Drittlandtransfers und das Zusammenspiel von DSGVO und Data Act.

Allein dieser unvollständige Themenüberblick über die aktuelle Ausgabe zeigt, wie vielfältig und spannend das Wissens- und Aufgabenspektrum von Datenschutzbeauftragten ist. Dies erfordert – vielleicht mehr noch als in vielen anderen Berufen – lebenslanges Lernen. Als BvD begleiten wir Sie nach Kräften dabei, neuerdings auch mit einer kostenlosen telefonischen Erstberatung in datenschutzrechtlichen Fragen. Weitere Informationen hierzu finden Sie im Mitgliederbereich unserer Website.

Ich wünsche Ihnen eine anregende Lektüre.

Ihr

Thomas Spaeing
BvD-Vorstandsvorsitzender

INHALTSVERZEICHNIS

IM FOKUS

Eine neue Epoche?
Die BvD-Verbandstage in Berlin diskutierten über Cyberangriffe und technischen Datenschutz.
Christina Denz, Jürgen Hartz 6

Kennzeichnungspflichten für KI aus Perspektive der Ethik
Sechs Argumente für die bewusste Trennung von menschlicher und KI-generierter Kommunikation.
Jessica Heesen 10

Digitalisierung im Gesundheitswesen
Datenschutz behindert nicht die Digitalisierung im Gesundheitswesen, sondern ebnet ihr den Weg.
Bernd Schütze, Prof. Dr. Klaus Pommerening 14

Interview mit Max Schrems
Im Gespräch mit den BvD-News fordert Max Schrems stärkere Kontrollen bei DSGVO-Verstößen und spricht über die Rolle der DSB. 18

DATENSCHUTZRECHT

Datenschutzrechtliche Verkehrssicherungspflicht – ein Novum?
Die DS-GVO betrachtet den gesamten Lebenszyklus der Verarbeitung personenbezogener Daten und ist deshalb von einer „Datenschutzrechtlichen Verkehrspflicht" geprägt.
Dr. Jens Eckhardt, Dr. h. c. Marit Hansen 20

Was Datenschützer über das Strafrecht wissen müssen
Die DSGVO droht drakonische Geldbußen bei Datenschutz-Verletzungen an. Doch vielen DSB fehlt es an relevanten Kenntnisse, um auf das neue Datenschutzsanktionsrecht angemessen reagieren zu können.
Dr. Eren Basar 28

Bestandsdatenauskunft nach dem TTDSG
Welche Befugnisse haben Strafverfolgungsbehörden bei der Bestandsdatenauskunft nach TTDSG und wie unterscheiden sich diese vom US-amerikanischen Datenschutzniveau?
Matthias Lachenmann 32

DATENSCHUTZPRAXIS

Datenverarbeitung in einem Drittland
Wie lässt sich ein Data Transfer Impact Assessment durchführen?
Regina Mühlich, Bernd Schütze 36

Schritt für Schritt zum Datenschutz
Mit der Website „Datenschutz für Kleinunternehmen" unterstützt die Stiftung Datenschutz kleine Betriebe und Selbständige dabei, sich datenschutzkonform aufzustellen.
Carsten Laumann, Kirstin Vedder 40

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-gs@bvdnet.de

Fotos (sofern nicht anderweitig ausgewiesen)
123RF, Adobe Stock,
BvD-Veranstaltungen: Dirk Lässig

Lektorat
Frank Spaeing, Regina Mühlich

Anzeigen
Christina Denz

Kooperationen
Karsten Füllhaase
(bvd-news@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.

Data Act and GDPR
Issues, Risks and Measures Data Protection Officers need to be aware of.
Petra Miloschewitschova, Jiri Mnuk, Michal Nuliçek 44

AUFSICHTSBEHÖRDEN

KI und Datenschutz
Auch wenn allgemein Verhaltensregeln und Zertifizierungen zur Einhaltung rechtlicher Rahmenbedingungen einen sinnvollen Beitrag leisten können, benötigt KI einen vorgegebenen Rechtsrahmen.
Dr. Jan Wacke, Dr. Peter Nägele 48

GESELLSCHAFT

Rotkäppchen und das Datenschutzproblem
Kinderbuchautorin Tina Blase erklärt für den BfDI Informationsfreiheit und Datenschutz in vier Pixi-Büchlein.
Christina Denz 52

AUS DEM VERBAND

Austausch, Vernetzung, Sichtbarkeit
Viel Neues beim Europäischen Dachverbands EFDPO.
Karsten Füllhaase 54

Spannend und aufklärend: Jury vergibt die DAME 2022
Christina Denz 58

Kurz gefasst
Vorstand im Amt bestätigt 62
"Trusted Data Processor" im Überblick 62
BvD-Beratungshotline für Mitglieder gestartet 63
Linkttipps 63

REZENSIONEN

Ein Algorithmus hat kein Taktgefühl 64
Die digitale Transformation des Qualitätsmanagements 65
Entzauberung des Rechts auf informationelle Selbstbestimmung 66

TERMINE / SERVICE

Termine der Regionalgruppen und Arbeitskreise des BvD 68
BvD Partnership Program 69
BvD-Fortbildungen 70

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

EINE NEUE EPOCHE?

Wie KI und Cyberangriffe Datenschutzbeauftragte herausfordern

Christina Denz, Jürgen Hartz

Nicht nur Brüssel und seine Digitalgesetzgebung stellt Datenschutzbeauftragte in Europa vor neue Herausforderungen. Es ist die Digitalisierung selbst, jüngste Entwicklungen bei der Künstlichen Intelligenz (KI) und die wachsende Bedrohung für Unternehmen und Behörden vor Cyberattacken, die die Regelungen zum Datenschutz auf die Probe stellen. Wird es gelingen beim Datenschutz mit der rasanten Entwicklung mitzuhalten? „Können wir uns Datenschutz noch leisten?" lautete das Motto der 16. BvD-Verbandstage am 9. und 10. Mai in Berlin. «Wir müssen uns Datenschutz leisten», war die Antwort.

„KI betrifft auch Datenschutzbeauftragte" sagte BvD-Vorstandsvorsitzender Thomas Spaeing zum Auftakt der mit 300 Teilnehmenden bislang größten Veranstaltung des BvD in seiner Geschichte. Denn KI beschleunige Cyberangriffe auf öffentliche wie nicht-öffentliche Stellen. Dabei hätten Datenschutzbeauftragte eine wichtige Beratungsfunktion, gerade auch bei kleinen und mittleren Unternehmen. Denn nicht immer könnten diese sich eigene IT-Sicherheitsfachleute leisten.

Kritik an der ePA

Dabei hatte Thomas Spaeing insbesondere den Medizinbereich im Blick. Denn dort sorgt nicht nur die seit bald 20 Jahren geplante elektronische Patientenakte (ePA) für Debatten. Auch sogenannte Fütter-Roboter und andere intelligente Versorgungssysteme, robotergestützte Operationen oder automatische Diagnostiksysteme benötigen eine Vielzahl an personenbezogenen Daten.

Aber selbst elementarste Fragen, was mit den gesammelten Daten geschieht, wo sie gespeichert werden, wer Zugriff auf sie erhält und wie sie gesichert und verschlüsselt sind, sind bislang unbeantwortet. Aktuell winkt selbst die Ärzteschaft in Teilen ab, weil sie den Datenschutz der ePA nicht garantieren kann, wie Thomas Spaeing ausführte.

BvD-Vorstandsvorsitzender Thomas Spaeing

Kritik an der ePA äußerte auch IT-Security-Analyst Carl Fabian Lüpke alias Flüpke auf der Konferenz. Das bisherige Vorgehen bezeichnete er als «absolut haarsträubend», nicht der Datenschutz sei an der schleppenden Entwicklung schuld, «sondern Stümperei». Insbesondere kritisierte er, dass es für die privaten Krankenversicherungen keine Verpflichtung zur zentralen Speicherung der Patientendaten gibt, sondern ausschließlich für Kassenpatienten. «Privacy kostet in Zukunft», sagte Flüpke.

IT-Security-Analyst Carl Fabian Lüpke alias Flüpke

Cybercrime nutzt Schwachstellen in den Systemen

Dabei ist der Datenschutz nur eine Seite der Medaille. Die andere Seite ist die Cyberkriminalität. Sind Systeme von Krankenhäusern, Praxen oder Unternehmen nicht sicher aufgesetzt sind sie leicht von Kriminellen zu knacken. Schwachstellen im System sind das Einfallstor für Malware, Trojaner und Viren, warnen Fachleute wie Haya Shulmann.

> *„IT-Sicherheit rückt bei uns stärker in den Fokus, weil die Notwendigkeit dafür da ist. Die Sicherheit bei Datenschutz und der IT spielen bei uns aktuell die größte Rolle. Wir versuchen, unsere Kunden auf die Gefahrenlage aufmerksam zu machen. Aber für viele ist die Bedrohungslage noch zu weit weg. Trotzdem bemerken wir eine steigende Nachfrage zum Thema Datensicherheit. Helfen würde eine Statistik, die zeigt, wie real für viele Unternehmen Cyberkriminalität ist."*
>
> Susanna van Boxem, Sachverständigenbüro Mülot

Deshalb appelliert die international anerkannte Wissenschaftlerin vom Fraunhofer SIT in Darmstadt vor allem an kleine und mittelständische Betriebe ihre IT-Systeme regelmäßig auf Schwachstellen zu untersuchen. Shulman weiß um die Schwierigkeiten des Mittelstandes. „Oft gibt es dort Experten für Datensicherheit, da ist der Datenschutzbeauftragte der einzige, der sich mit Daten auskennt", sagte sie in ihrer per Video übertragenen Key Note zum Auftakt der BvD-Verbandstage.

Laut Shulman haben sich Cyberangriffe seit der Corona-Pandemie und der dadurch ungeordnet explodierten Digitalisierung in allen Sektoren und Bereichen potenziert. Dabei wachse aktuell wieder die Bedeutung von E-Mail, die Hacker auf Social-Media-Plattformen wie LinkedIn und Facebook und mit Hilfe von Infostealer-Softwares gleich inklusive Passwörter erbeuteten. Die Daten wandern dann als Ware ins Darknet.

CYBERCRIME-AS-A-SERVICE

Cybercrime ist mittlerweile ein professionelles Geschäft. In der Underground Economy gibt es zahlreiche Marktplätze, auf denen illegale Güter wie Drogen, Waffen oder Kinderpornografie, gestohlene Daten und Identitäten, aber auch Dienstleistungen zur Begehung von Cyber-Straftaten angeboten werden, also Cybercrime-as-a-Service.

Der moderne Hacker programmiert seinen Angriff nicht mehr selber, sondern nutzt ein vielfältiges Angebot aus dem Darknet um quasi per Baukasten die Attacke zu konfektionieren. Dafür erhält er mitunter sogar Garantie. Beim Kauf von gestohlenen Kreditkarten beispielsweie wird zugesichert, dass diese über einen bestimmten Zeitraum nicht gesperrt sind – wenn doch, gibt es kostenlos Ersatz.

Polizeilich erfasst sind gemeldete Cybercrime-Fälle bis 2021. Laut Statista erreichten die missbräuchliche Nutzung von Telekommunikationsdiensten, das Ausspähen und Abfangen von Daten, Daten-Hehlerei, Fälschung und Täuschung im Rechtsverkehr sowie Datenveränderung/Computersabotage einen neuen Rekord. 127.137 solcher Straftaten waren 2021 gemeldet worden.

Die Dunkelziffer, so schätzen Experten, dürfte höher liegen. Denn manch angegriffenes Unternehmen zahlt das geforderte Lösegeld in der Hoffnung schnell wieder die Daten und damit die Arbeitsfähigkeit zurückzuerlangen.

Details zur Cyberkriminalität in Europa bis zum Jahr 2022 erläutert die Agentur der EU für Cybersicherheit (ENISA) in ihrem Bericht *Threat Landscape* 2022.

▶ enisa.europa.eu/publications/enisa-threat-landscape-2022

„Passwörter werden ein wichtiger Teil von Cyberkriminalität", sagt Shulman. „Die persönlichen Daten spielen eine immer wichtigere Rolle in diesem kriminellen Ökosystem". Es gebe im Darknet Millionen E-Mail-Adressen umfassende Listen.

Und dennoch würden etwa bei DAX-Konzernen und an Hochschulen – beide Bereiche untersuchte Shulman und ihr Team

dezidiert auf IT-Sicherheitsstrukturen – Passwörter mehrfach verwendet, von IT-Fachleuten wie von Studierenden und Mitarbeitenden. Schwachstellen gebe es aber auch bei Services und Ports, fand Shulman heraus. „Hier brauchen wir mehr Awareness", sagte sie.

Vor allem, dass E-Mails mittlerweile zum Einfallstor Nummer 1 für Cyberkriminelle geworden sind, schockte BvD-Vorstand Thomas Spaeing. Er wollte sich nicht ausmalen was zu erwarten sei, wenn Kriminelle KI-Systeme kaperten. «Und was passiert mit Geschäftsgeheimnissen unter KI», fragte er nach dem Vortrag von Shulman.

> *„Wir arbeiten als Anwälte eng mit Versicherern zusammen. Und dort laufen viele Anfragen ein, die sich nach Versicherungsschutz bei einem Cyberangriff informieren. Große Unternehmen orientieren sich am Cybersecurity Framework, das helfen will, die Infrastruktur gegen Angriffe robust zu machen. Bei kleinen Unternehmen ist das Bewusstsein für eine Prävention weniger ausgeprägt."*
>
> Thomas Kahl, Taylor Wessing

Cyber-Krimi in der Realität

Wirtschaftsprüfer und Rechtsanwalt Karl-Christian Bay und Datenschutz- und Informationssicherheitsberater Tobias Baader berichteten aus dem Inneren der Cyberattacke auf den Lebensmitteleinzelhändler tegut… gute Lebensmittel GmbH & Co. KG (tegut) im April 2021. Bay sitzt unter anderem im Beirat des Mittelständlers. Was er den Zuhörenden erzählte, verschlug ihnen fast den Atem. Obwohl tegut laut Bay bereits mit seiner IT-Infrastruktur und insbesondere der Organisation an sich gut aufgestellt war, und - Glück im Unglück, dass ein IT-Mitarbeiter sofort die Filialen abkoppelte, als er den Angriff bemerkte - durchlief das Unternehmen laut Bay alle Stadien einer klassischen Cyberattacke von der Verschlüsselung der Daten, über unzählige Erpressungsversuche, versuchte DDOS-Attacken, Veröffentlichung von Unternehmensdaten im Darknet und Trittbrettfahrer, die an der Attacke mitverdienen wollten.

Im Jahr der Attacke auf tegut explodierte laut Baader die Zahl der Ransomware-Angriffe um 435 Prozent. In der Folge des russischen Angriffskriegs auf die Ukraine stieg 2022 auch die Zahl der zielgerichteten Angriff, insbesondere DDOS-Attacken. Dabei schleusten die Angreifer mitunter so viel Traffic auf die Zielsysteme, dass die in die Knie gingen und nicht mehr erreichbar waren. Diesem Wahnsinns-Wachstum steht ein Mangel an ausgebildeten Fachleuten gegenüber: «Etwa drei Millionen Cyber-Fachkräfte fehlen», sagte Baader.

Ihm zufolge sind rund 95 Prozent der Cybersecurity-Vorfälle auf menschliches Versagen zurückzuführen: Ein Mitarbeiter öffnet eine mit Schadsoftware bestückte E-Mail, eine Mitarbeiterin wird auf eine gefälschte Seite geleitet und gibt dort Daten ein. «Wir müssen dringend in die sogenannte Human Firewall und in Trainings der Beschäftigten investieren», sagt Baader.

Das Vertrackte: Die Angreifer geben sich selten direkt zu erkennen, sodass der Angriff meist lange Zeit bis zum eigentlichen Impakt unbemerkt bleibt. Fachleute sprechen von der «stillen Phase», in dem die Täter bereits im gekaperten System agieren, Daten und Befugnisse abschöpfen, aber das System keine Anzeichen eines Angriffs erkennen lässt. Bei tegut ging es - typischerweise - in der Nacht los, von Freitag auf Samstag gegen 4:30 Uhr. «Das Unternehmen ist extrem gut aufgestellt gewesen, es gab Krisenstäbe, Notfallprogramme. Bis zum Frühstück waren alle informiert», sagt Bay.

Tegut entschied laut Bay, mit dem Vorfall in die Öffentlichkeit zu gehen und kein Lösegeld zu zahlen. Die zuständigen Ermittlungsbehörde, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die zuständige Datenschutzaufsichtsbehörde waren laut Bay eng eingebunden. Und dennoch: Wie viele Unternehmen tatsächlich Opfer von Angriffen werden, ist nicht klar. Denn manches Unternehmen zahlt die geforderte Summe in der Hoffnung, die Geschäfte bald wieder normal fortführen zu können. Denn ein Angriff kann gerade für kleine und mittelständische Unternehmen mitunter existenzgefährdend sein.

> *„Wir arbeiten mit kleinen und mittleren Unternehmen zusammen. Viele IT-Abteilungen haben sich nach unserer Erfahrung bereits auf mögliche Angriffe vorbereitet. Ich glaube auch, dass die meisten Verantwortlichen die Gefahren sehen. Der Beratungsaufwand zum Thema Cyberkriminalität hat deshalb bei uns nicht zugenommen. Jetzt muss es darum gehen, die Mitarbeitenden ebenfalls für mögliche Angriffe etwa über E-Mail zu sensibilisieren."*
>
> Stephan Eschenbacher, Eschenbacher IT-Consulting & Services

DIE BVD-VERBANDSTAGE WACHSEN: NEUER TEILNEHMER-REKORD IN BERLIN

Jürgen Hartz

Die 16. BvD-Verbandstage 2023 in Berlin waren die bislang größte Veranstaltung in der Geschichte des BvD. Rund 300 interne und externe behördliche wie betriebliche Datenschutzbeauftragte trafen sich zu Gesprächen und Diskussionen rund um aktuelle Themen des Datenschutzes. Dabei standen Praxisbeispiele und der technische Datenschutz im Vordergrund, nachdem die vergangenen Jahre vor allem juristische Fragen zur DSGVO die Themen der Tagungen bestimmten.

Unter den hochkarätigen Rednern waren neben dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Prof. Ulrich Kelber, der österreichische Datenschutzaktivist Max Schrems, die SPD-Datenschutzexpertin und Bundestagsabgeordnete Carmen Wegge sowie der frühere Chefredakteur der «Süddeutschen Zeitung», der Autor und Kolumnist Prof. Dr. Dr. Heribert Prantl.

Kelber bekräftigte gleich zu Beginn der Tagung seine Forderung nach einer Herstellerhaftung bei digitalen Anwendungen für Datenschutz. «Warum muss der Mittelstand für etwas verantwortlich sein, was Microsoft, Google und andere entwickeln», sagte er. Die Pflicht für „privacy by default & design" muss bereits beim Hersteller beginnen. Vielfach hat das nutzende Unternehmen gar keine Möglichkeit mehr auf grundlegende Sicherheitsmerkmale Einfluss zu nehmen, wenn sie nicht schon zu Beginn implementiert wurden.

Wegge zeigte sich optimistisch, dass die Regierungskoalition noch in der laufenden Legislatur das seit langem geplante Beschäftigtendatenschutzgesetz den Bundestag passieren werde. Anders als bei anderen Gesetzgebungsverfahren schaltete laut Wegge das Bundesarbeits- und Bundesinnenministerium den Stakeholderprozess vor die Ressortabstimmung. Dies solle helfen etwaige Widerstände im Vorfeld zu identifizieren und ein neuerliches Scheitern zu verhindern, führte Wegge aus. Bis Ende des Jahres soll dann der Referentenentwurf vorliegen.

Publizist und Autor Heribert Prantl beendete die BvD-Verbandstage mit einem eindringlichen Appell Datenschutz und Individualrechte stärker zu schützen. Gerade in der Corona-Pandemie habe die damalige Bundesregierung die Individualrechte kollektiviert. „Die Freiheitsrechte wurden klein und kleiner geschrieben", sagte Prantl. Künftig dürfe in Krisen das Parlament nicht umgangen werden. „Die Hürden für Grundrechtseingriffen müssen wieder höher gelegt werden", verlangte er.

Kritik übte er an der kürzlich verabschiedeten Verordnung, wonach die Konten von Bürgerinnen und Bürger mit dem Bundeszentralamt für Steuern verknüpft werden sollen. Die geplante Personen-Identifikationsnummer für Verwaltungen habe das Bundesverfassungsgericht bereits mehrfach als Negativbeispiel eines verfassungswidrigen Vorgehens verworfen, mahnte Prantl. Datenschutz, mahnte er zum Schluss, sei kein Bürgerrecht, sondern ein Grundrecht.

Wir danken unseren Event- und Medienpartner für ihre Unterstützung und die thematische Bereicherung der BvD-Verbandstage.

Die nächsten BvD-Verbandstage finden vom 14. bis 15. Juni 2024 in Berlin statt.

Ulrich Kelber

Max Schrems

Carmen Wegge

Heribert Prantl

Über die Autoren

Christina Denz
ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News".

Jürgen Hartz
ist stellvertretender Vorstandsvorsitzender des BvD e.V.

JESSICA HEESEN

KENNZEICHNUNGSPFLICHTEN FÜR KI AUS PERSPEKTIVE DER ETHIK

Sechs Argumente für die bewusste Trennung von menschlicher und KI-generierter Kommunikation

Neue Generationen von KI erstellen Medieninhalte und kommunizieren in menschenähnlicher Form. Für den Menschen wird es zunehmend schwierig zwischen solchen synthetischen Medien einerseits und menschlicher Kommunikation und Medienproduktion andererseits zu unterscheiden. Für den Aufbau kritischer Technikkompetenz, zur Wahrung der Integrität menschlicher Kommunikation und zum Schutz der Datenqualität sind KI-Kennzeichnungspflichten unabdingbar.

Anwendungen der Künstlichen Intelligenz (KI) kommen in den letzten Jahren zunehmend einem Versprechen nach, das schon lange mit der Entwicklung digitaler Techniken verbunden ist: Der Computer soll sich so natürlich wie möglich mit der Handlungswelt des Menschen verbinden.[1] Für eine nutzungsfreundliche und anschmiegsame Technik ist es charakteristisch die technischen Eigenschaften eines Artefakts aus dem menschlichen Bewusstsein verschwinden zu lassen. Gelingen kann dies unter anderem durch die Gestaltung einer intuitiven und menschenzentrierten Mensch-Computer-Interaktion, die es den Nutzerinnen und Nutzern ermöglicht mit einem informationstechnischen System ähnlich wie mit einer Person zu interagieren. Besonders hervorzuheben sind für diese menschenähnliche Kommunikation Sprachassistenzsysteme und KI-Sprachmodelle. Anwendungen wie ChatGPT, aber auch viele andere Dienste wie etwa für den Journalismus, den Bildungsbereich oder die Medizin sind dazu in der Lage anstelle des Menschen Medien- und Kommunikationsinhalte zu produzieren oder als Chatbot, teils mit menschlichem Antlitz, zur Verfügung zu stehen. Sie ermöglichen somit eine zweifache menschenähnliche Kommunikation: die Herstellung einer Interaktionssituation und die Generierung von synthetischen Medieninhalten.

Medieninhalte (Text, Bild, Audio und Video), die durch KI hergestellt worden sind, werden unter dem Begriff synthetische Medien zusammengefasst. Möchte man zum Ausdruck bringen, dass die solcher Art produzierten audio-visuellen Inhalte in täuschender Absicht hergestellt wurden, wird in der Regel der Begriff Deepfakes verwendet. Die Bezeichnung kommunikative künstliche Intelligenz[2] betont den interaktiven Aspekt der Kommunikation zwischen Mensch und KI.

Gerade weil es in der öffentlichen und privaten Kommunikation zunehmend schwierig wird zu erkennen, welche Inhalte von KI erzeugt wurden, kommt immer wieder die Forderung auf synthetische Medien und KI-gesteuerte Kommunikation verpflichtend zu kennzeichnen. Aber auch abgesehen von KI-Anwendungen, die menschliche Kommunikation und Medienproduktion imitieren, gibt es gute Gründe generell eine Kennzeichnungspflicht für die Verwendung von KI einzuführen. Dies betrifft besonders dringlich Dienste, die über Lebenschancen entscheiden wie etwa die Nutzung von KI in der Personalauswahl oder für die Zulassung zu Bildungsinstitutionen, oder KI-Systeme, die für Recht und Strafverfolgung verwendet werden und entsprechend im KI-Regulierungsvorschlag der europäischen Kommission[3] als Hochrisikoanwendungen eingeordnet werden. Auch die europäische Datenschutzgrundverordnung gibt Transparenzpflichten für KI vor, macht aber keine konkreten Vorgaben zur Kennzeichnung von synthetischen Medien. Ebenso erfordert die journalistische Berufsethik generell die Kennzeichnung manipulierter Bilder, hat sich in dem für Deutschland einschlägigen Pressekodex jedoch

[1] Weiser, Mark. 1991. "The Computer for the 21st Century." Scientific American 09/1991: 66-75

[2] Dehnert, M., & Mongeau, P.A. (2022). Persuasion in the age of artificial intelligence (AI): Theories and complications of AI-based persuasion. Human Communication Research. https://doi.org/10.1093/hcr/hqac006.

[3] Europäische Kommission (2021): Proposal for a Regulation laying down harmonised rules on artificial intelligence. (Artificial Intelligence Act), 21.04.2021 https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

noch nicht zu synthetischen Medien geäußert. International entstehen derzeit erste gesetzliche Vorgaben insbesondere zum Umgang mit Deepfakes, die aber insbesondere für China zeigen, wie ambivalent Regelungen sein können, die mit der Kontrolle von Medieninhalten einher gehen und die Meinungsäußerungsfreiheit einschränken könnten.[4]

Im Folgenden werden in einem Aufriss aus Perspektive der philosophischen Ethik sechs Argumente für die Kennzeichnung der Verwendung von KI angeführt.

Gründe für KI-Kennzeichnungspflichten

1. Transparenz

Transparenz ist ein Standardelement der Anforderungen, die im Rahmen zahlreicher Kodizes zur Ethik der KI veröffentlicht wurden.[5] Transparenz ermöglicht, dass Personen, die von KI-Entscheidungsvorbereitungen betroffen sind oder mit KI-Systemen arbeiten, zu informierten Entscheidungen kommen. Fragen der Transparenz betreffen üblicherweise Offenlegungspflichten in Bezug auf die verwendeten Algorithmen oder die Daten, mit denen Modelle trainiert werden. Konsequenterweise bezieht sich Transparenz aber auch auf die Kennzeichnung der Verwendung von KI an sich und auf die Kennzeichnung von durch KI erstellte Medieninhalte. Transparenz ist eine notwendige Voraussetzung dafür, dass Rechtsverletzungen identifiziert und korrigiert werden können. Transparenz über den Einsatz von KI ist zudem eine grundlegende Voraussetzung zur Ermöglichung gesellschaftlicher Debatten und zum Aufbau von Vertrauen in KI-gestützte Anwendungen.[6]

2. Medienmündigkeit

Als Reaktion auf die Herausforderungen einer stark durch Medienkommunikation strukturierten Gesellschaft wurden und werden immer wieder Forderungen nach Medienkompetenz oder in aktuelleren Terminologien Medienmündigkeit und Computer Literacy laut. Medienmündigkeit als Fähigkeit, verantwortungsvoll und selbstbestimmt mit Medien umzugehen[7], erfordert Klarheit über die Kommunikationssituation, die Kommunikationspartner und die beteiligten Unternehmen und Institutionen. Sie kann nur dann wirksam werden, wenn durch Kennzeichnungen deutlich wird, was als Betrachtungsobjekt besonders in den Fokus rücken sollte, und wenn die Ausbildung kritischer Medienkompetenz durch Kennzeichnung unterstützt und geachtet wird.

[4] Hine, Emmie/Floridi, Luciano (2022), New deepfake regulations in China are a tool for social stability, but at what cost? Nature Machine Intelligence, Vol. 4, July 2022, 608-610, https://doi.org/10.1038/s42256-022-00513-4

[5] AIEIG (Artificial Intelligence Ethics Impact Group) (2020), From Principles to Practice. An interdisciplinary framework to operationalise AI ethics, VDE/Bertelsmann Stiftung, Creative Commons 2020, https://www.ai-ethics-impact.org/resource/blob/1961130/c6db9894ee73aefa489d6249f5ee2b9f/aieig---report---download-hb-data.pdf; Jobin, Anna/Ienca, Marcello/Vayena, Effy (2019), The global landscape of AI ethics guidelines. Nature Machine Intelligence, Vol 1, 2019 | 389–399, https://doi.org/10.1038/s42256-019-0088-2

[6] Mohammed, Sedir et al. (2023). Ein Glossar zur Datenqualität (1.2). Zenodo. https://doi.org/10.5281/zenodo.7702426

[7] Bleckmann, Paula (2020): Medienmündig. Klett-Cotta, Stuttgart, 7. Aufl. 2020

3. Integrität menschlicher Kommunikation

Menschliche Kommunikation dient nicht alleine der Informationsvermittlung, sondern hat eine elementare Bedeutung für Identitätsausbildung und Verständigung.[8] Menschliche Kommunikationsbeziehungen sind von normativen Erwartungen geprägt, die sowohl die Form als auch den Inhalt der Kommunikation betreffen. Solche Erwartungen beziehen sich im Allgemeinen auf die Wahrheit des Gesagten, die Wahrhaftigkeit der Gesprächspartnerin (dass sie sagt, was sie meint) und die normative Richtigkeit (also unsere Vorstellungen vom sozial und moralisch Gebotenen).[9] Um diesen Erwartungshorizont aufrecht zu erhalten, ist es wichtig, dass Individuen durch Kennzeichnungen zwischen menschlichen und maschinellen Interaktionspartnern unterscheiden können. Ist dies nicht der Fall, entstehen „Interaktionssurrogate", die dem Bedürfnis nach authentischer Kommunikation widersprechen. Den Ansprüchen an menschliche Kommunikation ist es geschuldet Interaktionsbeziehungen nicht als *instrumentelles* Wechselverhältnis zu konzipieren. In KI-Anwendungen wird jedoch eine vermeintlich menschliche Kommunikation als Mittel zum Zweck der Steuerung eines Dienstes genutzt und sollte entsprechend transparent gemacht werden. Aus ethischer Perspektive sind die Achtung der Selbstzweckhaftigkeit und Unverfügbarkeit der Interaktionspartner prägender Hintergrund von Kommunikation und Verständigung. Die daraus resultierenden besonderen Kriterien für das Gelingen von Verständigung, wie etwa die wechselseitige Anerkennung der Gleichberechtigung der Kommunizierenden, sollten jederzeit klar erkennbar nur menschlichen Personen vorbehalten bleiben.

4. Normative Anforderungen an öffentliche Kommunikation

Öffentliche Kommunikation ist ein Kernelement der Demokratie, insbesondere weil sich die Bestimmung des Gemeinwohls aus dem öffentlichen Diskurs legitimiert.[10]

Wenn Medieninhalte durch KI produziert werden, kann dies bei den Rezipierenden ein generelles Misstrauen gegenüber Medienkommunikation erzeugen. Da es in der öffentlichen, politischen Kommunikation um die Verständigung zwischen Menschen geht, kann die Verwendung von KI Befürchtungen vor Manipulation und Desinformation hervorbringen und zu genereller Zurückhaltung in Bezug auf die aktive und passive Teilhabe an öffentlicher Kommunikation führen. Dem kann durch einen transparenten Umgang mit den Funktionen von KI für die jeweiligen Medienerzeugnisse entgegengewirkt werden.[11]

5. Datenqualität

Große KI-Sprachmodelle (Large Language Models, LLM) basieren in der Regel auf Daten, die aus öffentlich zugänglichen Internetquellen gewonnen werden. Gleichzeitig produzieren allgemeine KI-Sprachmodelle und auch spezifische KI-Anwendungen für den Journalismus selbst Texte und Bilder sowie Audio- und Videobeiträge. Um die Qualität von Trainingsdaten zu sichern und um die Reproduktion falscher Informationen und Daten zu vermeiden, sollte nicht nur für Personen, sondern auch für die maschinelle Datenverarbeitung erkennbar sein, ob ein durch KI erzeugter Inhalt vorliegt. Maschinenlesbare Kennzeichnungspflichten sind eine notwendige Bedingung, um eine selbstreferenzielle Nutzung von KI-Quellen zu verhindern.

6. Objektivierbarkeit von Technikverhältnissen

Anwendungen kommunikativer KI lassen den Menschen leicht vergessen, dass es sich bei der „Kommunikationspartnerin" um statistisch arbeitende Sprachmaschinen handelt. Zahlreiche Studien aus den vergangenen Jahrzehnten zeigen, dass Menschen zum Anthropomorphisieren von Techniken neigen, vor allem sobald sie eine menschenähnliche Gestalt haben oder eben ähnlich („emotional") wie Menschen kommunizieren.[12] Gerade der sensible Bereich der Mensch-Computer-Interaktion kann beispielhaft und prägend für die Vorstellung einer Gesellschaft vom „richtigen" Umgang mit technischen Artefakten sein. Zu einem reflektierten Technikverständnis, das immer auch Kritik und Kontrolle impliziert, gehört Techniken als Artefakte zu objektivieren und sich ihres künstlichen Charakters bewusst zu sein. Um keine falschen Erwartungen in Hinsicht auf Verständigung zu wecken (oder Menschen in Verhaltensmuster parasozialer Interaktion zu zwingen, siehe 3.), sollte KI-gesteuerte Kommunikation jederzeit als solche erkennbar sein.

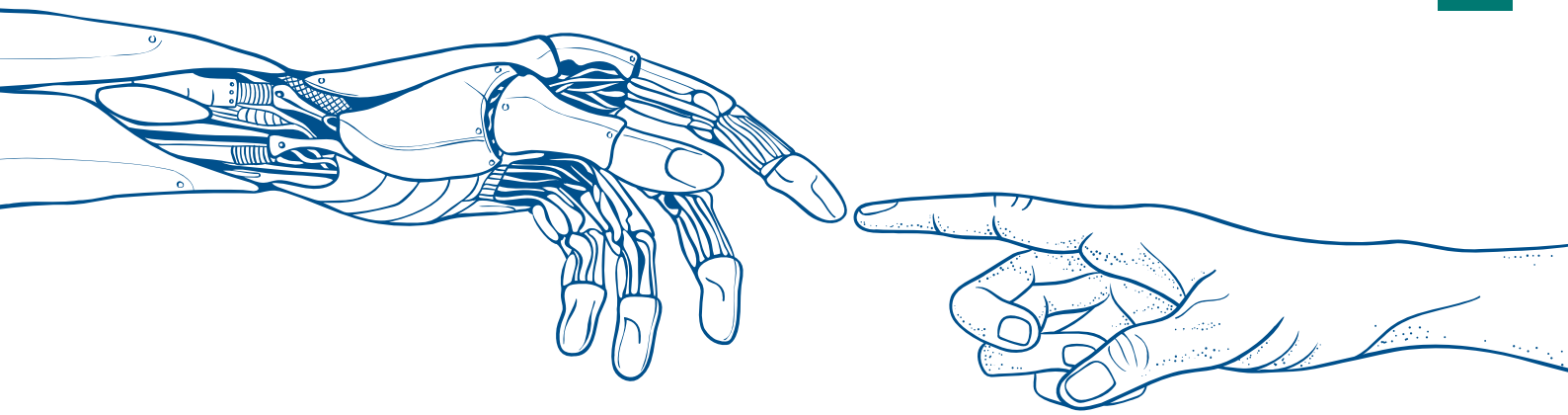
[8] Mead, George Herbert: Mind, Self and Society. Chicago/London 1934

[9] Habermas, Jürgen (1997): Theorie des kommunikativen Handelns. Bd. I: Handlungsrationalität und gesellschaftliche Rationalisierung, Frankfurt a. M., 2. Aufl. 1997, 148 ff.

[10] Habermas, Jürgen (2022): Ein neuer Strukturwandel der Öffentlichkeit und die deliberative Politik. Berlin, 3. Auflage

[11] Heesen, Jessica et al. (Hrsg.): KI-Systeme und die individuelle Wahlentscheidung – Chancen und Herausforderungen für die Demokratie. Whitepaper aus der Plattform Lernende Systeme, München 2021, S. 25. DOI: https://doi.org/10.48669/pls_2021-1

[12] Lee, J.-E. R., & Nass, C. I. (2010). Trust in computers: The Computers-Are-Social-Actors (CASA) paradigm and trustworthiness perception in human-computer communication. In Trust and technology in a ubiquitous modern environment (S. 1–15). IGI Global. https://doi.org/10.4018/978-1-61520-901-9.ch001



Praktische Möglichkeiten für Kennzeichnungen

Für die Kennzeichnung von KI bieten sich ganz unterschiedliche Möglichkeiten an. Sie sollten von ihrem Zweck her und entsprechend der Adressatenkreise konzipiert werden. Für die Kennzeichnung gegenüber Personen bzw. in der Medienkommunikation bieten sich Hinweise wie *standardisierte Zeichen am Produkt oder zurückhaltendere Angaben in den Metadaten* an, die darüber Auskunft geben, ob z. B. ein Bild bearbeitet wurde. Das Spektrum der zu kennzeichnenden KI reicht hier von dem Hinweis auf Filter bis hin zu synthetischen Medien, die durch KI kreiert wurden. Die Verursacher böswilliger oder in manipulativer Absicht verbreiteter Deepfakes werden ihre Produkte nicht kennzeichnen (vielmehr gibt es im Sinne der „Lügner-Dividende" zunehmend auch die Tendenz authentische Inhalte als Deepfakes zu deklarieren).[13] Hier kann es umgekehrt helfen, zumindest für kritische Medieninhalte oder Chatanwendungen, *Authentizitätszertifikate* zu erstellen, ähnlich wie sie jetzt bereits für die Identitätsprüfung für Social Media Accounts vorzufinden sind. Zusätzlich können mit Hilfe von (zurzeit noch unzuverlässig arbeitenden) Detektionssystemen für Inhalte, die durch generative KI erstellt wurden, Kennzeichnungen erfolgen. In diesen Fällen geht es dann nicht um eine freiwillige Kennzeichnung durch die jeweils Verantwortlichen, sondern um eine *maschinelle Identifikation KI-generierter Inhalte*.

Im Bereich der *maschinenlesbaren Kennzeichnungen* befinden sich Wasserzeichen für Erzeugnisse aus generativer KI in Diskussion und Entwicklung.[14] Während sich die oben aufgeführten Lösungen vor allem auf kommunikative Inhalte beziehen, sind auch weitergehende Forderungen nach der Kennzeichnung der Nutzung von KI für das Kuratieren von Inhalten und – losgelöst von Medienprodukten – generell für die Beteiligung von KI an Entscheidungsprozessen für unterschiedliche Anwendungen wie öffentliche Verwaltung oder Medizin in der Diskussion.[15]

FAZIT

Aus den sechs genannten Argumenten wird deutlich, dass KI-Kennzeichnungspflichten kein bürokratischer Selbstzweck sind, sondern ein Mittel zur Verwirklichung zentraler gesellschaftlicher Ziele wie transparente, rechtskonforme und kritische Techniknutzung sowie integre und vertrauenswürdige (öffentliche) Kommunikation. Selbsterklärungsleistungen gehören in einer demokratischen Gesellschaft zu den Qualitätsmerkmalen technischer Systeme. Sie sind ein wichtiger Beitrag zur Beherrschung und wertgeleiteten Entwicklung von KI und damit eine Voraussetzung für gesellschaftliche Akzeptanz und ethische Akzeptabilität. Aus diesen Gründen sind (auch automatisiert lesbare) Kennzeichnungen für KI-generierte Medienprodukte Bestandteil normativer Forderungskataloge zum Umgang mit KI.

Über die Autorin

PD Dr. Jessica Heesen
ist Leiterin des Forschungsschwerpunkts Medienethik und Informationstechnik am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen. Sie ist Autorin zahlreicher Veröffentlichungen zu ethischen Fragen der Nutzung von digitalen Medientechniken und zur Ethik der Künstlichen Intelligenz. Sie ist Leiterin verschiedener Forschungsprojekte zum Themenfeld Digitalisierung, darunter zur Sicherheit von Kindern online, zu Problemen der KI-Trainingsdatenqualität oder zu Privatheit in digitalen Handlungswelten.

▶ uni-tuebingen.de/de/15781

[13] Pawelec, Maria (2022), Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions, Digital Society 1:19, https://doi.org/10.1007/s44206-022-00010-6

[14] Kirchenbauer, John et al. (2023), A Watermark for Large Language Models, vorveröffentlicht in: arXiv, https://arxiv.org/pdf/2301.10226.pdf

[15] Europäische Kommission (2021): Proposal for a Regulation laying down harmonised rules on artificial intelligence. (Artificial Intelligence Act), 21.04.2021, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

DIGITALISIERUNG IM GESUNDHEITSWESEN

Das Datenschutzrecht ebnet den Weg

Bernd Schütze, Prof. Dr. Klaus Pommerening

Immer wieder wird „der Datenschutz" als wesentlicher Grund dafür angeführt, dass Deutschland bei der Digitalisierung des Gesundheitswesens „international den Anschluss verloren" hat. Schaut man hingegen genauer hin, sind es in der Regel andere Gründe, insbesondere die über die Jahre gewachsenen Strukturen im deutschen Gesundheitswesen, wo jede der Interessengemeinschaften der Selbstverwaltung im Gesundheitswesen entsprechend ihrem gesetzlichen Auftrag eher die eigenen Ziele als das Allgemeinwohl verfolgt. „Datenschutz" wird in diesen Fällen oft vorgeschoben, um die dahinter stehenden Interessen zu verschleiern.

Um dies zu verdeutlichen, wird im Folgenden zunächst dargestellt, was „Datenschutz" eigentlich bedeutet und wie Datenschutz in Beziehung zur Weiterentwicklung der Digitalisierung und speziell der medizinischen Forschung steht und diese fördert.

Datenschutz und Forschung: Zwei Grundrechte im Spannungsverhältnis

Die informationelle Selbstbestimmung aller Menschen beruht rechtlich in Deutschland auf Art. 1 und 2 des Grundgesetzes: Das allgemeine Persönlichkeitsrecht umfasst laut Bundesverfassungsgericht den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten. Einschränkungen dieses Rechts auf „informationelle Selbstbestimmung" sind zulässig, aber nur im überwiegenden Allgemeininteresse. Auch Forschung wird im Grundgesetz adressiert: Nach Art. 5 Grundgesetz sind Kunst und Wissenschaft, Forschung und Lehre frei. Im Europarecht findet sich der Schutz personenbezogener Daten (personenbezogenen Daten) in Art. 8 der Charta der Grundrechte, Forschung in Art. 13. Sowohl Datenschutz als auch Forschung stellen somit Grundrechte dar.

Das Datenschutzrecht ist nicht deckungsgleich mit dem Recht auf informationelle Selbstbestimmung. Und eine Fehlinterpretation wäre, dass es die Verarbeitung von personenbezogenen Daten verhindern soll. Das Datenschutzrecht dient vielmehr dem Ausgleich zwischen den Interessen der mit der Verarbeitung der personenbezogenen Daten befassten staatlichen und privatwirtschaftlichen Stellen auf der einen Seite, sowie den Interessen betroffener Personen auf der anderen Seite: Nur durch die im Datenschutzrecht verankerten organisatorischen und verfahrensrechtlichen Vorkehrungen wird eine Verarbeitung von personenbezogenen Daten erst ermöglicht, das heißt, ohne Datenschutzrecht ist eine Verarbeitung personenbezogenen Daten grundsätzlich nur mit Einwilligung möglich. Voraussetzung ist aber, dass es eine rechtliche Grundlage für die Verarbeitung gibt, die dem rechtsstaatlichen Gebot der Normenklarheit genügt und dabei zugleich die Verhältnismäßigkeit des Grundrechtseingriffes gegenüber den betroffenen Personen hinreichend berücksichtigt. Insbesondere müssen betroffene Personen die Tragweite einer Verarbeitung auf Grundlage des Gesetzes für sich selbst begreifen und einschätzen können.

Wie das Bundesverfassungsgericht feststellte: **Einschränkungen des Rechts** auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig. Aktuell liegt der Nachweis, dass beispielsweise ein medizinisches Forschungsvorhaben im **überwiegenden Allgemeininteresse** erfolgt, bei den forschenden Personen selbst. Dies erweist sich als schwierig, da keine Kriterien dafür vom Gesetzgeber vorgegeben werden.

Natürlich liegt nicht jedes Forschungsvorhaben im überwiegenden Allgemeininteresse. Daher müssen seitens des Gesetzgebers nachvollziehbare Kriterien benannt werden, wann bei medizinischer Forschung von einem überwiegenden Allgemeininteresse ausgegangen werden kann, zum Beispiel:

- Das Forschungsvorhaben adressiert eine Verbesserung der medizinischen Versorgung für einen signifikanten Anteil von an Erkrankung leidenden Menschen, auch bei seltenen Erkrankungen.
- Das Forschungsvorhaben könnte die Kosten einer Behandlung spürbar reduzieren und somit das Sozialwesen entlasten.

Digitalisierung des Gesundheitswesens und medizinische Forschung

Sekundärnutzung von Gesundheitsdaten aus Krankenhäusern oder auch Arztpraxen bedeutet, dass die Daten über den unmittelbaren Behandlungszusammenhang hinaus ausgewertet werden. Am Beispiel der COVID-19-Pandemie wurde deutlich, wie wichtig es wäre zeitnah einen bevölkerungsweiten Überblick über das Krankheitsgeschehen zu erhalten, und seien es nur zuverlässige Fallzahlen. Aber auch viele weiteren Nutzungen von Gesundheitsdaten sind denkbar bis hin zum Training von KI-Methoden, die den diagnostischen Prozess unterstützen sollen. In den Worten des Wissenschaftsrats: „Die Digitalisierung von Gesundheitsforschung und Versorgung eröffnet völlig neue Möglichkeiten des wissenschaftlichen Erkenntnisgewinns über Entstehungsmechanismen von Krankheiten und Wirksamkeit von Therapien sowie damit zusammenhängend völlig neue Möglichkeiten der öffentlichen und individuellen Gesundheitsvorsorge, der zielgenauen Diagnose, der personalisierten Behandlung, des Zugangs zu hochqualitativen, innovativen Versorgungsangeboten."

Nun handelt es sich bei diesen Gesundheitsdaten um personenbezogene Daten, die sogar zusätzlich besonderem Schutz unterliegen:

- Einmal definiert die DS-GVO diese als „besondere Kategorien" personenbezogenen Daten, die besonders strengem Schutz unterliegen, was eine weitere Verwendung an sehr strenge Auflagen knüpft.
- Zum anderen unterliegen sie der beruflichen Schweigepflicht der Behandelnden, die im Strafrecht festgeschrieben ist und eine Weitergabe an Personen verbietet, die nicht dem direkten Behandlungsteam angehören.

Damit bewegen wir uns in einem Bereich, wo verschiedene Gesetze und Grundrechte im Spannungsverhältnis miteinander stehen. Juristisch gesprochen bedeutet das, dass verschiedene Rechtsgüter gegeneinander abgewogen werden müssen: Die Persönlichkeitsrechte, die grundgesetzlich garantiert und durch das Datenschutzrecht konkretisiert werden, die Pflicht des Staates die Gesundheit seiner Bürger bestmöglich zu schützen, und die Wissenschaftsfreiheit, die hier dem medizinischen Fortschritt dienen soll und somit auch im öffentlichen Interesse steht. Dieses Spannungsverhältnis aufzulösen kann nicht die Aufgabe des einzelnen Forschungsprojekts sein. Vielmehr sind möglichst klare Kriterien seitens des Gesetzgebers und Leitlinien etwa von Fachgesellschaften unverzichtbar.

Die Digitalisierung des Gesundheitswesens und der Aufbau einer Dateninfrastruktur mit möglichst umfassendem Zugriff auf Gesundheitsdaten wie etwa Patientenakten soll zu einem Fortschritt der medizinischen Versorgung beitragen: Man könnte aktuelles Krankheitsgeschehen bevölkerungsweit überblicken und damit die Ressourcensteuerung im Gesundheitswesen optimieren, man könnte Zusammenhänge zwischen Behandlungsmethoden und Therapieerfolgen zeitnah erkennen, man könnte die Leistungen verschiedener Einrichtungen mit dem Ziel der medizinischen Qualitätssicherung vergleichen, man könnte wissensbasierte Therapieunterstützung anbieten, man könnte mühelos geeignete Probanden und Probandinnen für klinische Therapiestudien finden, und vieles mehr. Soweit jedenfalls die Wunschvorstellungen, die aber noch weitgehend utopisch sind. Der Weg zur Umsetzung ist mühsam. Diese Mühe wird oft „dem Datenschutz" angelastet. Dieser Vorwurf ist nicht ganz ohne Substanz, bildet aber, wie eingangs dargestellt, nur einen sehr kleinen Teil der Realität ab. Sicher, Datenschutzanforderungen erschweren einige allzu naive Ansätze. Viele andere Hindernisse sind aber mindestens genauso gravierend. Beispielsweise wird häufig vom „grünen Tisch" eine Digitalisierung im Gesundheitswesen geplant, ohne dass eine entsprechende Fach- und Sachkenntnis der bei den Leistungserbringern vorhandenen Workflows vorliegt, was dann zur Folge hat, dass die von Gesetzgebern bzw. deren Organen geplanten Digitalisierungsbemühungen eher zu Behinderungen bei der Patientenversorgung führen als diese zu unterstützen. Auch die mangelnde Datenqualität behindert die Digitalisierung: Aus Datenhalden kann man nur dann zuverlässiges Wissen extrahieren, wenn diese Daten korrekt, sorgfältig eingegeben und gepflegt sowie möglichst verzerrungsfrei sind.
Die nächsten massiven Hindernisse auf dem Weg in eine brauchbare Dateninfrastruktur erschweren oder verhindern sogar die übergreifende Auswertung: Auf der technischen Ebene sind Systeme nicht interoperabel, es kostet große Mühe ihnen Daten zu entlocken. Und auf der Datenebene sind die Daten aus verschiedenen Systemen nicht kompatibel, es mangelt an syntaktischer und semantischer Interoperabilität, an Standards und Normen – die nicht nur definiert, sondern auch eingehalten werden müssen. Besonders kontraproduktiv ist, dass viele relevante Daten noch gar nicht digital, sondern auf Papier erfasst werden. Und dort, wo Daten digital erfasst sind, sind die Daten oftmals nicht automatisiert auswertbar.

Schließlich wird der Fortschritt auch durch Vorbehalte bei den Mitwirkenden behindert, die Zusatzaufwand bei der Anpassung eingeübter und funktionierender Prozesse scheuen.

Insgesamt ist die Digitalisierung des Gesundheitswesens ein hochkomplexer Prozess, der nur langsam vorankommt und erhebliche Kosten nach sich zieht und neben großen Chancen auch Risiken birgt. Regelungen des Datenschutzrechts lassen viele Wege zur Datennutzung im öffentlichen Interesse offen, verlangen aber – und hier verursachen sie tatsächlich Mühe – große Sorgfalt und besondere Maßnahmen, insbesondere auch zum Schutz der Patientinnen und Patienten. Für die beabsichtigte Nutzung muss die Erforderlichkeit nachvollziehbar begründet sein – was bei medizinischen Fragestellungen und Projekten nicht allzu schwer fallen sollte – und die Angemessenheit der Maßnahmen dokumentiert werden. Insbesondere auf Datensparsamkeit ist zu achten, und das bedeutet Prozessabläufe und die dabei benötigten Daten sorgfältig zu definieren.

Handlungsbedarf

Auf der rechtlichen Seite sollte Folgendes getan werden:

1) Homogenisierung des nationalen Datenschutzrechts

Versorgung im Krankenhaus wird in jedem Bundesland anders geregelt, jedes Bundesland hat spezielle Datenschutzregelungen. Diese unterschiedlichen, bundeslandspezifischen Datenschutzregelungen behindern sowohl die (länderübergreifende) Patientenversorgung wie auch die medizinische Forschung. Grundsätzlich könnte der Bundesgesetzgeber ein Gesetz zur medizinischen Forschung erlassen, welches auch einen Erlaubnistatbestand zur Nutzung von zur Patientenversorgung erhobenen personenbezogenen Daten beinhaltet. Dieses Bundesgesetz stünde gegebenenfalls jedoch in Konkurrenz zu den jeweiligen landesgesetzlichen Krankenhausgesetzen, die die Verarbeitung von zur Versorgung erhobener Patientendaten abschließend regeln. Aus Gründen der Rechtsunsicherheit würden Verantwortliche die Patientendaten daher nicht für Forschungsvorhaben bereitstellen, welche nicht in Einklang mit dem jeweiligen Landesrecht stehen. Sollen die länderübergreifende Versorgung ermöglicht und die medizinische Forschung gefördert werden, so müssen die deutschen Bundes- und Landesgesetzgeber eine Homogenisierung der datenschutzrechtlichen Regelungen herbeiführen.

2) Forschung mit Biomaterial und anderen Daten, welche Informationen von Dritten beinhalten

Insbesondere ist eine (harmonisierte) nationale Regelung zur Verarbeitung von solchen Daten, welche die Verarbeitung unabhängig von der Einwilligung regelt, wünschenswert. Derartige Daten wie beispielsweise Biomaterial oder vererbbare Erkrankungen, welche prinzipiell auch Daten über verwandte Personen wie beispielsweise Kinder, Eltern, Enkel enthält, sind im Rahmen der Vorgabe der DS-GVO mittels Einwilligung kaum zu verarbeiten, da eine Einwilligung immer nur für die eigenen Daten, nicht aber für die Daten Dritter gegeben werden kann.

3) Definition, wann von einem „überwiegenden Allgemeininteresse“ ausgegangen werden kann

Forschungsvorhaben müssen durch eine unabhängige Institution bewertet und Daten bei Vorliegen eines überwiegenden Allgemeininteresses für das Forschungsvorhaben ausdrücklich von der Institution freigegeben werden. Dabei müssen Sanktionen vorgesehen sein, das heißt, Akteure der Institution haften für ihre Entscheidung zum Beispiel durch entsprechende Strafvorschriften für unlautere Handlungen wie beispielsweise Entscheidung einzelner Personen bei Befangenheit aufgrund einer eigenen Erkrankung.

4) Forschung mit nicht-anonymen Daten erleichtern

Einerseits ist eine Anonymisierung im medizinischen Kontext bei einer ausreichend großen Datenmenge kaum realisierbar. Andererseits ist eine Anonymisierung in diversen Forschungsprojekten auch nicht umsetzbar, weil Rauschen und Vergröberungen der Daten Ergebnisse verfälschen, zum Beispiel wenn Beobachtungen am Randbereich erforderlich sind, um Fragestellungen wie „Warum sprechen 0,5 Prozent der Patienten nicht auf die Gold-Standard-Therapie an“ bearbeitet werden sollen und ein konkreter Zusammenhang und nicht nur statistische Angleichungen zur Forschung erforderlich sind.

5) Schutz durch Sanktionen, auch für Forscher

Es sollten Strafvorschriften für Forscher bei Datenmissbrauch durch den Gesetzgeber eingeführt werden. Dies kann angelehnt an § 203 StGB erfolgen, jedoch sollte dies kein reines Antragsdelikt sein:

1. Betroffene Personen erfahren vielleicht nichts vom Missbrauch, können daher also keinen Antrag stellen.
2. Verbraucherschutzverbände, Selbsthilfegruppen und ähnliche Organisationen sollten Anträge stellen können, da die Forschung ja im entsprechenden Allgemeininteresse erfolgt und diese Gruppen entsprechende Interessen der betroffenen Personen vertreten.
3. Medizinische Forschung, insbesondere KI, braucht häufig Daten von sehr vielen Patienten, das heißt, es ist auch ein entsprechendes Interesse des Volkes an Aufklärung vorhanden. Daher sollte eine Staatsanwaltschaft in derartigen Fällen selbstständig, das heißt, ohne vorherige Antragstellung, ermitteln dürfen.

Hindernisse, die durch Datenschutzregelungen bedingt sind und beseitigt werden sollten, sind vor allem der föderale Wirrwarr im gesetzgeberischen Bereich, allgemein das komplexe Regulierungsgeflecht, sowie fehlende gesetzliche Erlaubnistatbestände wie zum Beispiel ein Forschungsdatengesetz, Registergesetze, die Etablierung eines Forschungsgeheimnisses (mit entsprechenden Sanktionen bei Verstößen) – ohne dabei das Regulierungsgeflecht noch weiter aufzublähen! Insbesondere muss Bundes- und Landesrecht unter Beachtung der Vorgaben des Grundgesetzes und der Grundrechtecharta der Europäischen Union miteinander abgestimmt werden, damit endlich deutschlandweit einheitliche Rahmenbedingungen für im überwiegenden Allgemeininteresse liegende medizinische Forschung geschaffen werden, die auch Bestand haben und nicht bei der ersten Klage vom Bundesverfassungsgericht als für nicht vereinbar mit geltendem Recht bewertet werden, wie es in den letzten 20 Jahren mit einer Vielzahl von hastig verabschiedeten Gesetzen geschah.

Auf der technischen Seite müssen Krankenhaus- und Praxissysteme oder allgemeiner elektronische Patienten- und Gesundheitsakten den Aufbau einer Dateninfrastruktur unterstützen. Dazu gehören:

- Interoperabilität, insbesondere mit Datenintegrationszentren und Registern oder einem Gesundheitsforschungsdatenportal, aber auch zwischen den Systemen von Gesundheitsdienstleistern wie Krankenhäusern, Arztpraxen oder Apotheken; dies umfasst unter anderem
  - einheitliche technische Schnittstellen, welche sektorenübergreifend einen Austausch ermöglichen,
  - aber auch Definitionen, die eine syntaktische und semantische einheitliche Interpretation beim Austausch von Gesundheitsdaten gewährleisten,
- Werkzeuge zur datenschutzgerechten Sekundärnutzung wie Anonymisierungs- und Pseudonymisierungstools,
- Unterstützung verteilter Auswertungen,
- Elektronische Verfügbarkeit von abgestuften und differenzierten Einwilligungen.

IT-Sicherheitsanforderungen werden zwar auch durch den Datenschutz definiert, sind aber davon völlig unabhängig essenziell für alle beteiligten Stellen des Gesundheitswesens zwingend einzuhalten.

FAZIT

- Unter den vielen Hindernissen auf dem Weg zur Digitalisierung des Gesundheitswesens ist der Datenschutz im Vergleich zu anderen Problemen eher weniger entscheidend.
- Im Gegenteil – das Datenschutzrecht zeigt Wege, wie mit personenbezogenen Daten umgegangen werden kann.
- Ernst genommener Datenschutz ist außerdem eine wesentliche Voraussetzung, um das Vertrauen der Öffentlichkeit in die Digitalisierungsprozesse zu gewinnen.
- Die mit der Umsetzung von Datenschutzmaßnahmen betrauten Einrichtungen des Gesundheitswesens und insbesondere deren IT-Personal müssen durch klare gesetzliche Regelungen, leicht verständliche Leitlinien, unkompliziert funktionierende und sicher einsetzbare Infrastruktur sowie nachvollziehbare Musterlösungen unterstützt werden.
- Um diese Erleichterungen zu schaffen, sind der Staat als Gesetz- und Geldgeber und die medizinischen Fachgesellschaften als Ideengeber in der Pflicht.

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 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.

Prof. Dr. Klaus Pommerening
leitete bis zu seiner Pensionierung Ende 2011 die Abteilung Medizinische Informatik an der Universitätsmedizin Mainz. Davor war er Professor für Mathematik an den Universitäten Mainz und Heidelberg und forschte unter anderem zu Telematikplattformen in der Medizin. Über 20 Jahre war er Sprecher der Arbeitsgruppe „Datenschutz“ bei der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF e.V.) und publizierte unter anderem zu Kryptographie, Datenschutz und medizinischer Informatik.

Klaus Pommerening starb im Februar 2023, die vorliegende Kooperationsarbeit ist einer seiner zuletzt verfassten Beiträge.

„WIR MÜSSEN IN EINE ART DURCHSETZUNGSKULTUR SWITCHEN“

Max Schrems ist Vorstandsvorsitzender der 2017 von ihm gegründeten Organisation noyb, mit der er gegen Datenschutzverletzungen von Unternehmen vorgeht. Die Initiative versteht sich als Europäisches Zentrum für Digitale Rechte und informiert über aktuelle Entscheidungen in Europa zu Datenrechtsverstößen.

Der österreichische Datenschutzaktivist Max Schrems ist spätestens seit dem von ihm und seiner Organisation noyb erstrittenem Urteil des Europäischen Gerichtshofes (EuGH) zum transatlantischen Datentransfer bekannt geworden. Vor knapp drei Jahren, am 19. Juli 2020, erklärten die Richter in Luxemburg das bis dato geltende EU-US Privacy Shield für ungültig. Aber auch die neuen Vereinbarungen zwischen EU und den USA bewertet Max Schrems kritisch. Über eine wahrscheinlich neue Klage und stärkere Kontrollen in Europa sprachen die BvD-News mit dem Datenschützer.

BvD-News: *Herr Schrems, Sie hatten ja bereits angekündigt, dass Sie vor dem Europäischen Gerichtshof auch gegen das neue EU-US-Datenschutzabkommen klagen wollen. Gibt es bereits eine Entscheidung, dass Sie tatsächlich dagegen gerichtlich vorgehen werden?*

Max Schrems: Davon gehen wir aktuell aus. Noch fehlt die offizielle Schlussversion, theoretisch könnte sich also noch etwas ändern. Zudem muss ein Unternehmen meine Daten auf der neuen Grundlage zwischen Europa und den USA austauschen. Nur dann haben wir einen Betroffenen und können dagegen klagen. Aber nach dem aktuellen Stand gehen wir davon aus, dass wir wieder Klage einreichen werden.

BvD-News: *Sie haben diesen neuen Anlauf der EU als eine bewusste Verletzung rechtsstaatlicher Prinzipien bezeichnet. Aus welchen Gründen halten Sie das neue Vorhaben bis dato für nicht gesetzeskonform?*

Max Schrems: Das Abkommen ist politisch gewollt, was an sich okay ist, aber soweit wir sehen können gibt es einfach keine rechtliche Grundlage dafür, weil es im US-amerikanischen Recht keine wirklichen Änderungen gegeben hat. Die neue Executive Order wird zwar als Lösung gefeiert. Aber im Vergleich zur PPD-28 davor steht da größtenteils das Gleiche drin. Ob das juristisch Substanz hat wagen wir zu bezweifeln. So zu tun als ob jetzt alles neu wäre, das halt ich schon für ein bisschen verlogen.

BvD-News: *Wie müsste aus Ihrer Sicht eine Lösung aussehen, um den transatlantischen Datenverkehr wieder zu nutzen?*

Max Schrems: Langfristig bräuchten wir ein Agreement, in dem demokratische Staaten sagen, dass beide Seiten die gleichen Rechte haben. Das Lustige ist ja: Auf beiden Seiten des Atlantiks sind wir uns einig, dass die NSA-Überwachung verfassungswidrig ist – solche Überwachung wäre ja auch ein Verstoß gegen den vierten Verfassungszusatz in den USA. Der Unterschied liegt darin, dass die Amerikaner der Meinung sind, dass diese Grundrechte nur für US-Bürger gelten und nicht für Ausländer. Ohne ein Anerkenntnis, dass auch Ausländer Rechte haben können werden wir nicht weit kommen. Die einzige Lösung wäre hier gegenseitig ein Mindestmaß an Schutz zu garantieren.

BvD-News: *Schauen wir nach Europa. Wo liegen denn hier aus Ihrer Perspektive die größten Herausforderungen?*

Max Schrems: Das war und ist das Thema Durchsetzung. Nach fünf Jahren DSGVO stehen die Gesetze zwar auf dem Papier. Aber die Rechtsdurchsetzung ist noch sehr überschaubar. Wie können Datenschutzbeauftragte in einem Unternehmen die Einhaltung der Gesetze durchsetzen wenn es keine Konsequenzen gibt? Am Anfang war von hohen Strafen und vier Prozent des Umsatzes die Rede. Aber die Realität ist, dass solche Strafen nur in Ausnahmefällen verhängt werden. Die Unternehmen lernen also, dass sie bei DSGVO-Verstößen davonkommen und diese sich sogar auszahlen. Wir haben leider die ursprüngliche abschreckende Wirkung hier völlig verloren.

BvD-News: *Das bedeutet, Aufsicht und Kontrollen müssen in den europäischen Staaten verstärkt werden?*

Max Schrems: Wir müssen in eine Art Durchsetzungskultur switchen. Gerade in Deutschland gibt es eine Praxis, dass Unternehmen und Aufsicht sehr eng zusammenarbeiten. Damit wird die Aufsicht oft schon zur Rechtsberatung auf Kosten der Steuerzahler. Betriebe werden bei Verstößen erst mal verwarnt und aufgefordert den Verstoß bitte abzustellen. Das ist sehr außergewöhnlich im Recht. Wenn ich falsch parke, muss ich auch eine Strafe zahlen und werde nicht aufgefordert zukünftig nicht mehr falsch zu parken. Beim Datenschutz haben wir eine Kultur, wo man praktisch immer eine Extra-Einladung bekommt sich doch bitte mal an die Gesetze zu halten. Das war am Anfang noch verständlich, aber nach insgesamt sieben Jahren seit Verabschiedung der DSGVO versteht den laxen Umgang kein Mensch mehr. Die Bürger verstehen auch nicht, warum sie Strafe bekommen, wenn sie ihre Steuern nicht zahlen, aber Großkonzerne beim Datenschutz noch nicht mal eine Verwarnung bekommen. Da hilft nur eine klassisch abschreckende Strafe.

BvD-News: *Wie können wir sicherstellen, dass der Datenschutz in Europa robust bleibt?*

Max Schrems: Auf dem Papier ist der Datenschutz in Europa robust. Wir haben mit der DSGVO ein Gesetz, in dem alles da ist, Rechte, Pflichten und auch Strafen. Aber es fehlt die Exekutive. Die EU-Länder haben ja jeweils prozessrechtliche Eigenheiten entwickelt, so dass in manchen EU-Staaten die nötigen Verfahren einfach torpediert werden. Bei der 1,2-Milliarden-Strafe gegen Facebook durch die irische Behörde beispielsweise haben wir drei Mal die Behörde verklagt, bis sie endlich eine Entscheidung getroffen hat. Aber wenn ich als Betroffener drei Mal eine Behörde verklagen muss, um eine in erster Instanz eine Entscheidung zu bekommen, dann ist das System kaputt. Die EU arbeitet an einer Verfahrensharmonisierung. Die meisten Datenschutzbeauftragten haben es ja meist nur mit einer Behörde in ihrem Land zu tun. Wir von noyb haben mit über 40 Behörden zu tun. Das geht schon so weit, dass wir zum Beispiel in Polen Akteneinsicht nur vor Ort nehmen können und die Akten mit den Handy fotografieren müssen, weil es keinen Kopierer gibt. Oder in Bayern, wo die Akteneinsicht für Betroffene im Datenschutz ausgenommen ist. Das ist Schikane und da hat man das Gefühl, dass das, was Europa beschlossen hat, national wieder unterminiert werden soll.

BvD-News: *Wie ließe sich Datenschutz in Deutschland besser durchsetzen?*

Max Schrems: Deutschland ist beim Datenschutz eigentlich sehr stark. Die Aufsichtsbehörden haben im Vergleich zu anderen EU-Ländern viele Ressourcen. Europaweit bekommen die Aufsichtsbehörden circa 300 Millionen Euro pro Jahr, Deutschland erhält davon ein Drittel des Budgets. Aber dann stellen wir uns die Frage, ob da auch für ein Drittel des Datenschutzes in Europa ein Resultat erreicht wird. Da müssen die Behörden einfach effizienter werden und beispielsweise Prozesse automatisieren. Websites können automatisch gescannt und Beschwerden automatisch geschrieben und zugestellt werden. Dass die Datenschutzaufsichtsbehörden noch manuell jeden Fall behandeln und Anschreiben tippen und teils nicht mal in der Lage sind technische Dateien zu öffnen, so dass wir Screenshots schicken müssen, da merkt man, dass was passieren muss.

BvD-News: *Welche Rolle sehen Sie für betriebliche und behördliche Datenschutzbeauftragte in Europa und in Deutschland?*

Max Schrems: In Deutschland ist es für Betroffene zwar schon schwierig genug ihre Rechte beim Datenschutz durchzusetzen. Aber im Unterschied zu anderen EU-Ländern gibt es hier schon lange den gesetzlich verankerten Datenschutzbeauftragten. In anderen EU-Staaten gibt es diese Tradition nicht. Da wollen die meisten Datenschutzbeauftragten primär ihr Unternehmen schützen und die Aufsichtsbehörden möglichst fern halten. Die ursprüngliche Idee, dass der Datenschutzbeauftragte für Datenschutz und die Rechte der Betroffenen sorgt, nehmen wir in Europa nur selten wahr. Deswegen hatte ich immer dafür plädiert dass man so eine externe Kontrolle ähnlich einer Rechnungsprüfung etabliert. Nur so wäre es halbwegs abbildbar, dass Datenschutzbeauftragte unabhängig agieren und nicht unter dem direkten Einfluss der Geschäftsführung stehen.

▶ noyb.eu/en

MAX SCHREMS

Max Schrems ist österreichischer Jurist, Autor und Datenschutzaktivist. Er konnte mit seiner Klage vor dem EuGH das transnationale Safe-Harbor-Abkommen zwischen der EU und den USA und später den EU-US Privacy Shield beenden. Er ist Gründer und Vorstandsvorsitzender der NGO NOYB, die sich der Durchsetzung von Datenschutzrechten verschrieben hat.

Das Interview führte

Christina Denz

ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News“.

DR. JENS ECKHARDT, DR. H. C. MARIT HANSEN

DATENSCHUTZRECHTLICHE VERKEHRSSICHERUNGS-PFLICHT – EIN NOVUM?

Die DS-GVO ist – anders als das BDSG und viele anderen Gesetze – kein Sammelsurium von Einzelregelungen für verschiedene Fragestellungen. Beim Lesen und Anwenden der DS-GVO wird deutlich, dass sie von einem Ansatz geprägt ist, den wir als ***Datenschutzrechtliche Verkehrssicherungspflicht*** *verstehen und – soweit ersichtlich erstmalig[1] – unter diesem Begriff diskutieren.*

1. Die Datenschutzrechtliche Verkehrssicherungspflicht

Der DS-GVO liegt zugrunde, dass von jeder Verarbeitung personenbezogener Daten ein Risiko für die Rechte und Freiheiten der betroffenen Person ausgeht. Es gibt demnach keine risikofreie Verarbeitung personenbezogener Daten.[2] Die DS-GVO reagiert hierauf jedoch nicht mit einem absoluten Verbot der Verarbeitung personenbezogener Daten, sondern – und insoweit über das BDSG-alt und die Datenschutzrichtlinie 95/46/EG hinausgehend – mit einer Vielzahl von Regelungen, (neben dem Verbot mit Erlaubnisvorbehalt) die das Risiko beherrschbar machen sollen.

Grob betrachtet formuliert die DS-GVO einzelne Anforderungen über den gesamten Lebenszyklus der Verarbeitung: von der Bewertung der Zulässigkeit vor der Verarbeitung über die Beherrschung des Risikos während der Verarbeitung bis hin zur Reaktion bei Verletzung der Sicherheit. Vertiefend betrachtet reihen sich die Regelungen Artt. 5, 12 ff., 22, 24, 25, 28, 29, 32, 33, 34, 35, 36, 44 DS-GVO wie Perlen an einer Schnur auf und haben alle gemeinsam, dass sie den Verantwortlichen (und zum Teil auch den Auftragsverarbeiter) dazu zwingen, technische und organisatorische Maßnahmen zu ergreifen, um entsprechend der Maßgabe der jeweiligen Norm das in dieser adressierte Risiko zu beherrschen. Als zentrale Regelung – möglicherweise aufgrund der fehlenden Bußgeldbewehrung nicht immer hinreichend beachtet – bringt Art. 24 DS-GVO das zum Ausdruck.

[1] Soweit ersichtlich erstmalig verwendet in: Eckhardt, Sicherheit der Verarbeitung: Der Zweck heiligt nicht die Mittel!, Datenschutz PRAXIS, Heft August. 2023 (im Erscheinen)

[2] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen, 26.04.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

In ihrer Gesamtschau ist die DS-GVO also von einer – durch uns so bezeichneten – *„Datenschutzrechtlichen Verkehrssicherungspflicht"* geprägt. Selbst wenn diese *Datenschutzrechtliche Verkehrssicherungspflicht* keine eigene haftungsbegründende Wirkung entfaltet, so beschreibt sie doch den gedanklichen Ansatz zur Umsetzung bzw. Einhaltung der Anforderungen der DS-GVO. Dieser Ansatz macht auch deutlich, wie Einzelregelungen der DS-GVO ineinandergreifen.

Die *Datenschutzrechtliche Verkehrssicherungspflicht* lässt sich so definieren: Wer durch seine Verarbeitung personenbezogener Daten eine Gefahrenquelle schafft, muss die erforderlichen Maßnahmen ergreifen, um die von seiner (jeweiligen) konkreten Gefahr ausgehenden Risiken für die betroffenen Personen zu beherrschen.[3]

Mit Risiko im Sinne der DS-GVO sind nicht nur IT-Sicherheitsrisiken wie Cyberangriffe oder Verlust oder Zerstörung von Datenträgern adressiert, sondern im Mittelpunkt stehen die Rechte und Freiheiten natürlicher Personen, die durch die Verarbeitung personenbezogener Daten beeinträchtigt oder verletzt werden können.[4] Der Begriff „Risiko" im Singular oder Plural kommt gleich 25-mal im Gesetzeswerk (und 43-mal in den zugehörigen Erwägungsgründen) vor.

Insbesondere in Bezug auf die zu treffenden technischen und organisatorischen Maßnahmen ist die Orientierung am Risiko vorgeschrieben. So heißt es in Art. 32 Abs. 1 DS-GVO, dass „der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen [treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Geregelt ist auch, dass im Rahmen einer Auftragsverarbeitung „alle gemäß Artikel 32 DS-GVO erforderlichen Maßnahmen" ergriffen werden müssen (Art. 28 Abs. 3 lit. c DS-GVO).

Eine Ausprägung der *Datenschutzrechtlichen Verkehrssicherungspflicht* der DS-GVO ist, dass die Pflicht zur Sicherheit der Verarbeitung sich nicht in Art. 32 DS-GVO erschöpft, sondern insbesondere auch in Artt. 33, 34 DS-GVO (sowie Art. 12 DS-GVO in Bezug auf danach zu erwartenden Auskunftsverlangen nach Art. 15 DS-GVO) zum Ausdruck kommt. Ebenso erfordert die DS-GVO jedoch, dass technische und organisatorische Maßnahmen zur Beherrschung von Risiken entsprechend den Vorgaben der DS-GVO wiederum selbst die Vorgaben der DS-GVO einhalten müssen, sodass insbesondere Artt. 5, 6, 12, 13, 14 DS-GVO auch auf die Verarbeitung personenbezogener Daten zur Umsetzung der Maßnahmen nach Artt. 32, 33, 34 DS-GVO anzuwenden sind.

BEISPIEL MALWARE-PRÜFUNG VON E-MAILS

Werden beispielsweise E-Mails mit mutmaßlichem Schadcode im Anhang in einen Quarantänebereich verschoben, sind in der Regel personenbezogene Daten des Absenders, des Empfängers und gegebenenfalls weiterer betroffener Personen, die etwa im E-Mail-Text oder im Anhang genannt werden, enthalten. Der Umgang mit einer solchen E-Mail kann zu weiteren Verarbeitungen personenbezogener Daten führen, z. B. wenn das Eingreifen eines Mitarbeiters aus der Systemadministration zum Verfügbarmachen der E-Mail dokumentiert, der Absender über einen mutmaßlichen Malware-Versand in Kenntnis gesetzt oder der Antivirus-Dienstleister über eine etwaige (Falsch-) Erkennung informiert wird. Auch das Unterlassen einer Malware-Prüfung kann weitere Verarbeitungen auslösen, beispielsweise wenn das IT-System infiziert wurde und Sofortmaßnahmen zum Retten der Daten und Vermeiden eines Datenabflusses getroffen werden müssen oder mit Hilfe einer forensischen Analyse der Infektionsweg bis zum Mitarbeiter-E-Mail-Postfach nachvollzogen werden soll, damit dieses Einfallstor für Malware geschlossen und der Weg der Ausbreitung versperrt wird. Es sind auch schon Ransomware-Angriffe bekannt geworden, bei denen die Angreifer interne Hilfe hatten[5] – und zwar nicht durch Nachlässigkeit, sondern mit Vorsatz einzelner Mitarbeitender. Sollten hier interne Untersuchungen in der Firma oder Behörde nötig oder die Daten an Strafverfolgungsbehörden übergeben werden, ist ebenfalls an den Personenbezug und das Datenschutzrecht zu denken.

Nach dem hier vertretenen Verständnis der *Datenschutzrechtlichen Verkehrssicherungspflicht* ist sie weder Synonym noch Ersetzung der in der DS-GVO in Einzelregelungen adressierten Risiken, sondern bedeutet deren gesamtheitliche

[3] Eckhardt, Sicherheit der Verarbeitung: Der Zweck heiligt nicht die Mittel!, Datenschutz PRAXIS, Heft August, 2023.

[4] DSK, Kurzpapier Nr. 18, 2018.

[5] Nayyar, Who Is Recruiting Your Workers? It Could Be A Hacker Group, Forbes, 11.10.2022, https://www.forbes.com/sites/forbestechcouncil/2022/10/11/who-is-recruiting-your-workers-it-could-be-a-hacker-group/

BEISPIEL: MELDE- UND BENACHRICHTIGUNGS-PFLICHTEN

Die Sicherheit der Verarbeitung findet im Lichte der *Datenschutzrechtlichen Verkehrssicherungspflicht* ihre Fortsetzung in Artt. 33, 34 DS-GVO. War das Risiko nicht ausreichend beherrscht, sodass es zu einer „Panne" im Sinne des Artt. 33, 34 DS-GVO kam, muss die so entstandene (ggf. weitere) Gefahrenquelle beherrscht werden, und die Verletzung dieser konkreten Ausprägung der *Datenschutzrechtlichen Verkehrssicherungspflicht* kann zur Haftung führen.

Doch insoweit gilt wiederum das für die Sicherheit der Verarbeitung Ausgeführte: Auch für die Verarbeitung personenbezogener Daten im Rahmen der Meldung und Benachrichtigung (sowie der Aufklärung) müssen die Vorgaben der DS-GVO berücksichtigt werden. Die Verarbeitung der Daten der betroffenen Personen zu deren Unterrichtung ist sicherlich durch Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO i. V. m. Art. 34 DS-GVO gerechtfertigt.

Anders stellt sich das schon wieder dann dar, wenn sich aufgrund vertraglicher Neben- oder Hauptpflichten oder (bspw. arbeitsrechtlicher) Fürsorgepflichten unterhalb der Schwelle des Art. 34 DS-GVO eine Informationspflicht an individuelle betroffene Personen ergibt oder sie einfach aus Fürsorge informiert werden sollen. Hier wird Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO nicht – jedenfalls nicht ohne Weiteres – in Betracht kommen.

Was ist aber mit der Benennung der Person, welche den „Panne" verursacht hat oder die – beispielsweise aufgrund eines Fehlversands irrtümlich und unverlangt – Kenntnis von den Daten erhalten hat? Mag sich dies gegenüber der Aufsichtsbehörde nicht so gravierend auswirken, muss bei einer Benennung gegenüber den nach Art. 34 DS-GVO zu benachrichtigenden Personen gut abgewogen werden. Wenn eine Herausgabe dieser Information bei der Benachrichtigung verneint wird, setzt sich diese Problematik fort, wenn die benachrichtigte Person die Benennung im Rahmen eines Auskunftsanspruchs verlangt.

Betrachtung, wenngleich die Ausprägungen jeweils in den Einzelregelungen enthalten sind.

2. Anforderung Sicherheit: was muss, was darf?

Die Sicherheit wird durch die DS-GVO als derart bedeutsam eingestuft, dass sie in den Kanon der Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 DS-GVO aufgenommen wurde: So regelt Art. 5 Abs. 1 lit. f DS-GVO, dass „personenbezogene Daten [...] in einer Weise verarbeitet werden [müssen], die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet". Sicherheit ist Pflicht.

Die Auswahl der technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO muss sich an dieser Vorgabe messen lassen – genauer: insbesondere an Art. 5 DS-GVO (siehe dort Abs. 1 lit. f: Grundsatz der „Integrität und Vertraulichkeit") und an Art. 24 DS-GVO mit dem Maßstab „Art, Umfang, Umstände und Zwecke der Verarbeitung" sowie „Eintrittswahrscheinlichkeit und Schaden der Risiken". Dabei ist auf die Gesamtschau der Maßnahmen abzustellen, die in ihrer Wirksamkeit zu bewerten ist (s. a. Art. 32 Abs. 1 lit. d DS-GVO).

2.1 Personenbezug bei Sicherheitsmaßnahmen

Zahlreiche infrage kommende technische und organisatorische Maßnahmen, die zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten dienen, sind wiederum mit einer Verarbeitung personenbezogener Daten verbunden oder erfordern sie sogar. Man denke nur an Zugriffskontrollsysteme, mit denen berechtigte Zugriffe autorisierter Mitarbeitender erlaubt und unberechtigte Zugriffe unterbunden werden sollen.

Auch beim Protokollieren[5] von schreibenden oder lesenden Zugriffen auf Dateien sowie von An- und Abmeldevorgängen an den IT-Systemen in Logdateien werden typischerweise personenbezogene Daten verarbeitet. Dies gilt ebenso für Backup und Restore, also für das Sichern und Wiederherstellen personenbezogener Daten. Scanner für Viren und andere Malware durchforsten die gespeicherten Daten – auch die personenbezogenen – nach schädlichem Code.

Zusammengefasst: Auf der einen Seite muss der Verantwortliche (und gegebenenfalls der Auftragsverarbeiter) geeignete technische und organisatorische Maßnahmen für einen angemessenen Schutz der personenbezogenen Daten treffen. Auf der anderen Seite können diese Maßnahmen mit einer Verarbeitung personenbezogener Daten verbunden sein, was – gar nicht überraschend – nur dann

[6] Vgl. spezifische Vorgaben zur und an die Protokollierung im Geltungsbereich Justiz und Inneres, wie in Teil 3 des BDSG in § 76 nach den Vorgaben von Art. 25 der Richtlinie (EU) 2016/680 umgesetzt.

zulässig ist, wenn wiederum die datenschutzrechtlichen Vorgaben eingehalten werden.

2.2 Rechtsgrundlage (nur) Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO?

Bei der Suche nach einer Rechtsgrundlage wird man – ebenfalls wenig überraschend – in der DS-GVO selbst fündig: Der Zweck der Verarbeitung ist die Gewährleistung der Sicherheit, wie sie in Art. 32 DS-GVO gefordert wird. Damit kann die Verarbeitung personenbezogener Daten in diesen Fällen auf Art. 6 Abs. 1 UAbs. 1 lit. c i. V. m. Art. 32 DS-GVO gestützt werden, denn „die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt".

Diese Regelung verdeutlicht, dass dies selbstverständlich nur für die Verarbeitung personenbezogener Daten im Rahmen der Erforderlichkeit gilt. Dies ist unionsrechtlich auszulegen und umfasst daher die Abwägung der Erfüllung der rechtlichen Pflicht zur Risikobeherrschung gegen die Rechte und Freiheiten der betroffenen Personen. Hier würde die Argumentation „Der Zweck Sicherheit heiligt die Mittel" nicht verfangen, sondern der Verantwortliche muss genauer hinschauen und differenzieren – insbesondere bezüglich des Sicherheitsniveaus, das dem mit der Verarbeitung zu dem primären Zweck einhergehenden Risiko angemessen ist. Es kommt auf die Beherrschung des konkreten Risikos an: Das Beherrschen eines hohen Risikos kann zusätzliche Maßnahmen erfordern, die andernfalls entbehrlich – also gerade nicht erforderlich – sind.[7]

Achtung: Die Rechtsgrundlage Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO greift nur im Zusammenspiel mit Normen, die den Anforderungen der Art. 6 Abs. 2, 3 DS-GVO genügen und insbesondere ausreichend spezifische Regelungen enthalten. Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO dürfte auf diese Weise in Verbindung mit den konkreteren Artt. 32, 33 und 34 DS-GVO zur Rechtsgrundlage taugen, doch werden nicht alle – nun ja doch des Öfteren abstrakt gehaltenen – Artikel in der Datenschutz-Grundverordnung in dieser Weise herangezogen werden können. So dürften hingegen z. B. Art. 5 und Art. 24 DS-GVO als nicht bestimmt genug einzustufen sein, um die Anforderungen aus Art. 6 Abs. 2, 3 DS-GVO zu erfüllen.

Kurzum: Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO kommt als Rechtsgrundlage zur Erfüllung der *Datenschutzrechtlichen Verkehrssicherungspflicht* jedenfalls nicht per se in Betracht.

2.3 Rechtsgrundlagen neben Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO

Die DS-GVO bietet weitere Rechtsgrundlagen, die je nach Konstellation für Sicherheitsmaßnahmen, die mit der Verarbeitung personenbezogener Daten verbunden ist, infrage kommen, wenn sich die Erforderlichkeit der Verarbeitung zum Zwecke der Sicherheit nicht allein aus den Anforderungen des Art. 32 DS-GVO ergibt.

Wird durch den Verantwortlichen gegenüber dem Mitarbeiter seines IT-Dienstleisters angeboten, anstatt ihn stets durch einen Beschäftigten abholen und begleiten zu lassen, den Einlass in die Räumlichkeiten durch eine Registrierung für ein Zugangstoken mit Protokollierung zu ersetzen, wird Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO als Rechtsgrundlage kaum in Betracht kommen. Dasselbe gilt, wenn eine Privatperson Dateien zum Zweck eines „Malware-Checks" durch einen Sicherheitsdienstleister überträgt und ihm auf diese Weise zugleich Informationen zur Verfügung stellt, damit dieser die Verbreitung oder neue Malware beobachten kann.

[7] Sog. „zusätzliche Maßnahmen" im Fall eines hohen Risikos, siehe DSK, Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, Version 3.0, 2022, Kapitel D3.4 „Bestimmung technischer und organisatorischer Maßnahmen insbesondere bei hohem Risiko", S. 54 ff., https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode-V30a.pdf; Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Kompendium, 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf, S. 3.

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

In diesen Fällen kommt die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a als Alternative in Betracht. Wie stets, ist die Einwilligung zwar im Prinzip eine mögliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten, aber es müssen zum einen die Voraussetzungen der Informiertheit und Freiwilligkeit erfüllt sein (Art. 4 Nr. 11, Art. 7 DS-GVO), zum anderen kann die Einwilligung von der betroffenen Person jederzeit mit Wirkung für die Zukunft widerrufen werden. Das gilt natürlich auch für eine Einwilligung in die Verarbeitung personenbezogener Daten zum Zwecke der Sicherheit. Nur, weil das Ziel „gut" ist, sind die Anforderungen der DS-GVO nicht ausgehebelt. Daher ist die Rechtsgrundlage Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO **(Einwilligung)** nur dann für den Verantwortlichen geeignet, wenn tatsächlich eine Wahlmöglichkeit für die betroffene Person besteht, ob deren Daten in diesem Zusammenhang verarbeitet werden. Zumeist wird dann diese Sicherheitsmaßnahme auch oder sogar primär im Interesse der betroffenen Person liegen.

Im Beschäftigtenverhältnis ist die Einwilligung an weitere Bedingungen geknüpft (siehe § 26 Abs. 2 BDSG).

Erteilt eine Privatperson einem Dienstleister den Auftrag, regelmäßig das Darknet nach den eigenen personenbezogenen Daten zu durchsuchen und bei Funden zu warnen, dürfte sich die entsprechende Datenverarbeitung nicht durch Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO rechtfertigen lassen. Dasselbe gilt, wenn Eltern Dienste von Anbietern einsetzen, um das Surf- und Chatverhalten ihrer Kinder zu überwachen.

Die Sicherheit der Verarbeitung personenbezogener Daten kann sich in bestimmten Konstellationen also auch aus einer Vertragspflicht (oder vertraglichen Nebenpflicht) ergeben und wäre dann auf Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO **(Vertragserfüllung)** beziehungsweise im Beschäftigtenverhältnis § 26 Abs. 1 UAbs. 1 S. 1 BDSG[8] zu stützen, wenn die personenbezogenen Daten des Vertragspartners[9] verarbeitet werden. Aus zivilrechtlicher Sicht birgt jeder Vertrag auch Schutzpflichten in Gestalt vertraglicher Nebenpflichten. Natürlich hat ein Verantwortlicher die personenbezogenen Daten der Beschäftigten seines Vertragspartners zu schützen, wenn er diese erhält, um über Ansprechpersonen, Weisungsberechtige, Kontaktstellen oder schlicht Vertragsunterzeichner informiert zu werden.

Eine besondere Konstellation der Nebenpflicht hat das OLG Dresden (Beschl. v. 05.09.2012, 4 W 961/12) dadurch begründet, dass es zu dem Ergebnis kam, dass ein E-Mail-Account eines ausgeschiedenen Mitarbeiters nicht ohne

[8] Vorbehaltlich der Auswirkungen der EuGH-Entscheidung vom 30.03.2023, Rs. C-34/21.

[9] Zum Beispiel ein Beschäftigter, ein Kunde oder auch Kinder, für die Sorgeberechtigte besondere Sicherheitsmaßnahmen verlangen.

Weiteres gelöscht werden dürfe, womit wohl als Nebenpflicht verfügbarkeits- und integritätswahrende Maßnahmen für die vorhandenen E-Mail-Nachrichten einhergehen. Spannend ist insbesondere in IT-Verträgen, was als Haupt- und Nebenpflicht in Bezug auf die personenbezogenen Daten des Auftraggebers einzuordnen ist.

Sicherheit ist in vielen Fällen ein berechtigtes Interesse des Verantwortlichen oder des Auftragsverarbeiters. So ist die typische Rechtsgrundlage für die meisten Fälle, die nicht dem Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO i. V. m. Art. 32 DS-GVO unterfallen, durch Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO **(Interessenabwägung)** gegeben. Auch in diesem Fall muss die Verarbeitung personenbezogener Daten durch die zu treffenden Sicherheitsmaßnahmen erforderlich sein. Die Abwägung, die der Verantwortliche durchführen muss, betrachtet die berechtigten Interessen des Verantwortlichen oder eines Dritten und prüft, ob nicht überwiegende Interessen, Rechte und Freiheiten der betroffenen Personen dieser Verarbeitung entgegenstehen. Über die berechtigten Interessen muss informiert werden (Artt. 13, 14 DS-GVO).

Art. 21 Abs. 1 DS-GVO sieht vor, dass betroffene Personen gegen die Verarbeitung ihrer Daten einen Widerspruch einlegen können und bei Vorliegen besonderer Gründe die Verarbeitung gegebenenfalls zu unterbleiben hat.

Zwei Besonderheiten: Erwägungsgrund 49 der DS-GVO stellt ein berechtigtes Interesse für die Verarbeitung personenbezogener Daten zur Gewährleistung der Netz- und Informationssicherheit fest, soweit diese unbedingt nötig und verhältnismäßig ist. Und: Für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung kommt Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht als Rechtsgrundlage infrage (Art. 6 Abs. 1 UAbs. 2 DS-GVO), sodass in der Regel auf Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO, u. U. auch auf lit. e, zurückzugreifen ist.[10]

Zwischenfazit

Ebenso wie Anforderungen zur Einhaltung der Pflichten geprüft werden müssen, müssen auch die dafür ausgewählten Maßnahmen – soweit sie mit der Verarbeitung personenbezogener Daten einhergehen – wiederum im Lichte der DS-GVO geprüft werden.

3. DS-GVO-Anforderungen an die Sicherheit

3.1 Sicherheit auch bei DS-GVO-Verarbeitungsprozessen

Die Datenschutz-Grundverordnung enthält Regelungen zu Datenverarbeitungsprozessen, die zusätzlich zu der originären vom Verantwortlichen gewollten Verarbeitung vorgesehen werden müssen, beispielsweise zur Umsetzung der Betroffenenrechte (Artt. 15-22 DS-GVO). So darf und muss der Verantwortliche personenbezogene Daten verarbeiten, wenn eine betroffene Person ihr Recht auf Auskunft nach Art. 15 DS-GVO wahrnimmt: Der Verantwortliche muss dabei gewährleisten, dass sie die sie betreffenden personenbezogenen Daten vollständig erhält, aber keine personenbezogenen Daten anderer bekommt. Das betrifft die Selektion der Daten; es betrifft aber auch den Umstand, dass sich der Verantwortliche ausreichend von der Berechtigung und damit der Identität der anfragenden Person überzeugen muss, damit nicht personenbezogene Daten an jemanden herausgegeben werden, der die Identität eines anderen vorgibt. Auch der Übertragungsweg bei der Herausgabe muss den Sicherheitsanforderungen der DS-GVO genügen.

Ähnliches gilt auch bei der Umsetzung der Benachrichtigungspflicht (Art. 34 DS-GVO) im Fall von Verletzungen des Schutzes personenbezogener Daten und einem voraussichtlich hohen Risiko für die betroffene Person: Gerade bei stattgefundenen Datenpannen ist dafür Sorge zu tragen, dass die Benachrichtigung keine

[10] In Erwägungsgrund 49 wird das „berechtigte Interesse" zum Zweck der Netz- und Informationssicherheit allerdings auch für Behörden genannt.

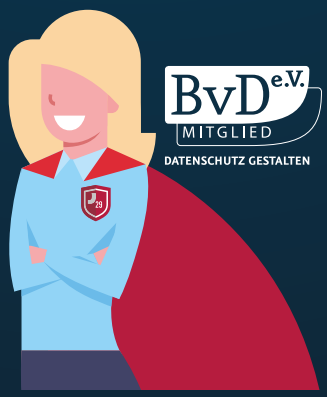
PRIVACYSOFT
Datenschutzmanagement as a Service

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

weitere Verletzung des Schutzes personenbezogener Daten auslöst.

3.2 Sicherheit ist kein Schön-Wetter-Thema

Die DS-GVO sieht vor, dass das Risiko für den gesamten Lebenszyklus der verarbeiteten personenbezogenen Daten beherrscht werden muss. Dies gilt auch für den Bereich der Sicherheit und die Gestaltung der Maßnahmen. Die Gewährleistung des dem Risiko angemessenen Sicherheitsniveaus kann zudem nicht als statisch betrachtet werden: Das Risiko erhöht sich beispielsweise dann, wenn die Eintrittswahrscheinlichkeit oder der mögliche Schaden steigen. Dies ist jeweils im Einzelfall zu bewerten. Es gibt deutliche Hinweise, dass zumindest der Faktor Eintrittswahrscheinlichkeit größer wird: Im Bereich der Informationssicherheit wachsen die Bedrohungen,[11] unter anderem mit neuen Angriffsmustern wie Supply-Chain-Attacks[12] oder Geschäftsmodellen wie Ransomware-as-a-Service.[13] Gleichzeitig sind über die letzten Jahre mit zunehmender Vernetzung, mobilem Arbeiten und Home-Office Angriffsvektoren hinzugekommen.

Für den Verantwortlichen bedeutet dies, dass er regelmäßig seine Sicherheitsmaßnahmen auf ihre Wirksamkeit überprüfen (Art. 32 Abs. 1 lit. d DS-GVO) und nachbessern muss. Dies betrifft Maßnahmen von Abwehr, Erkennung und Behandlung von Sicherheitsvorfällen. Bei der Frage der Zulässigkeit und der datenschutzkonformen Gestaltung müssen daher nicht nur die zu Beginn einmal implementierten Maßnahmen in ihrer Konfiguration betrachtet werden, sondern es geht im Sinne der *Datenschutzrechtlichen Verkehrssicherungspflicht* auch darum, dass die Rechtskonformität auch im Fehler- oder Eskalationsfall gewährleistet ist.[14] Solche Situationen können es nämlich notwendig machen, bisherige Maßnahmen anzupassen oder neue Maßnahmen hinzunehmen, die wiederum mit einer Verarbeitung personenbezogener Daten einhergehen: wenn beispielsweise zusätzliche Protokollierungen eingeschaltet oder weitere Auswertungen vorhandener Daten vorgenommen werden sollen, um einen laufenden Angriff zu erkennen und abzuwehren oder durch ein sogenanntes „Malware Post-Mortem" im Nachhinein Schwachstellen zu identifizieren und anschließend zu beseitigen. Bei einem Sicherheitsvorfall kann es auch nötig werden, spezialisierte Dienstleister einzubinden – selbstverständlich datenschutzkonform.

3.3 Es gilt die gesamte DS-GVO

Selbstverständlich gelten für die zu Sicherheitszwecken getroffenen Maßnahmen, die ihrerseits mit einer Verarbeitung personenbezogener Daten verbunden sind, alle datenschutzrechtlichen Anforderungen. Das bedeutet insbesondere:

- Die Gestaltung muss, wie stets, den Vorgaben der Artt. 24, 25 DS-GVO folgen und in diesem Zusammenhang auch die in Art. 5 DS-GVO formulierten Grundsätze einhalten. Beispielsweise dürfen nur die für die Zwecke der Sicherheit notwendigen personenbezogenen Daten (Datenminimierung) und nur so lange wie erforderlich (Speicherbegrenzung) verarbeitet werden. Auch der Grundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DS-GVO) ist bezüglich derjenigen personenbezogenen Daten, die zu Zwecken der Sicherheit verarbeitet werden, ernst zu nehmen, damit die Sicherheits-

[11] BSI, Die Lage der IT-Sicherheit in Deutschland 2022, Bonn, 2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf, S. 11.

[12] Ebd., S. 36.

[13] Ebd., S. 16.

[14] Hansen/Probst, Souveräne Sicherheit, Zero Trust und das Datenschutzrecht, DuD 10/2023 (im Erscheinen).

maßnahmen nicht selbst zum Sicherheitsproblem werden.[15]

- Es müssen die Informationspflichten nach Artt. 12-14 DS-GVO in ausreichender Detailtiefe und Verständlichkeit umgesetzt werden. Aber Achtung: In Bezug auf die Verarbeitung zu Zwecken der Sicherheit könnten genaue Informationen einem Angreifer in die Hände spielen.
- Der Verantwortliche muss in der Lage sein, die Betroffenenrechte auf Auskunft[16], Berichtigung, Löschung, Einschränkung der Verarbeitung, Übertragbarkeit (Artt. 15-20 DS-GVO) sowie im Fall von Profiling oder ähnlichen Verarbeitungen die Rechte nach Artt. 21, 22 DS-GVO zu erfüllen.
- Und: Natürlich umfassen die Dokumentationspflichten, die sich aus Art. 5 Abs. 2 DS-GVO sowie Art. 30 DS-GVO ergeben, auch die technischen und organisatorischen Maßnahmen zur Sicherheit, soweit sie personenbezogene Daten verarbeiten.

FAZIT

Die DS-GVO ist von der *Datenschutzrechtlichen Verkehrssicherungspflicht* als Grundansatz durchzogen. Das bedeutet, dass die Umsetzung der Vorgaben der DS-GVO sich nicht in einer Einzelbetrachtung von Einzelregelungen erschöpfen darf. Gleichzeitig sind – wie exemplarisch an der Sicherheit der Verarbeitung hinterfragt wurde – Maßnahmen zur Umsetzung der Vorgaben der DS-GVO selbst wiederum nicht befreit von den Anforderungen der DS-GVO. Der Zweck heiligt eben nicht die Mittel.

Aus der *Datenschutzrechtlichen Verkehrssicherungspflicht* heraus wird auch verständlich, dass die Beherrschung des Risikos, das von der Verarbeitung personenbezogener Daten für die Rechte und Freiheiten personenbezogener Daten ausgeht, nicht statisch ist. Die *Datenschutzrechtliche Verkehrssicherungspflicht* ist der DS-GVO immanent und aus dieser Perspektive nichts Neues – aber wohl erstmals so benannt.

Über die Autoren

Dr. h. c. Marit Hansen
Die Informatikerin ist Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

Dr. Jens Eckhardt
ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht sowie Datenschutz-Auditor (TÜV) und Compliance-Officer (TÜV). Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

[15] S. Kleine Anfrage „Erhebung biometrischer Daten und Nutzung von US-amerikanischen Datenbanken durch die Bundeswehr in Afghanistan", Bundestags-Drucksache 20/6270, 31.03.2023, https://dserver.bundestag.de/btd/20/062/2006270.pdf.

[16] Wie auch bei den Informationspflichten könnten aus Sicherheitssicht Einschränkungen geboten sein, s. ErwGr. 63 Satz 3 zu Art. 15 DS-GVO.

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

WAS DATENSCHÜTZER ÜBER DAS STRAFRECHT WISSEN MÜSSEN

Dr. Eren Basar

A. Einleitung

Spätestens seit der Entscheidung des Europäischen Datenausschusses (EDSA) zur Verhängung eines Bußgelds in Höhe von 1,2 Milliarden Euro gegenüber dem Unternehmen Facebook dürfte überdeutlich sichtbar geworden sein, dass das Sanktionsregime der DSGVO potenziell zu einem der gewichtigsten Haftungsrisiken für Unternehmen werden kann. Obgleich damit drakonische Geldbußen im Raum stehen, fehlt es bei vielen Datenschützern und Datenschutzbeauftragten in der Praxis an den relevanten Kenntnissen, um auf das neue Datenschutzsanktionenrecht angemessen reagieren zu können. Das betrifft auch diejenigen Datenschützer, die über eine juristische Ausbildung verfügen, was daran liegen mag, dass die Verteidigung von Unternehmen im Studium keine nennenswerte Rolle spielt. Der folgende Beitrag skizziert die für Datenschützer relevanten strafrechtlichen Basics, um für den Umgang mit Bußgeld- und Strafverfahren vorerst gewappnet zu sein.

B. Am Anfang und am Ende: die StPO

Der Umgang mit Bußgeld und Strafverfahren setzt am Anfang und am Ende Kenntnisse über die Strafprozessordnung (StPO) voraus. Als Datenschützer wird man jedenfalls keinerlei Wirkung für die Verteidigung des Verantwortlichen entfalten können, wenn man sich mit den dort verankerten Rechten für den Beschuldigten oder für das betroffene Unternehmen nicht vertraut macht. Das Verfahrensrecht für die Verhängung von Bußgeldern nach der DSGVO ergibt sich gemäß § 41 Abs. 2 S. 1 BDSG nach dem Gesetz über Ordnungswidrigkeiten (OWiG) und der StPO entsprechend. Das OWiG wiederum verweist für Bußgeldverfahren in § 46 Abs. 1 auf die *sinngemäße* Anwendung der StPO. Aus dieser zweifachen Verweisung folgen weitreichende Verteidigungsrechte, wozu unter anderem die Selbstbelastungsfreiheit, das Recht auf Zugang zu einem Rechtsbeistand, das Recht auf rechtliches Gehör und die Unschuldsvermutung gehören.[1] Der Verweis liefert zugleich die Grundlage für die rechtlichen Befugnisse der Aufsichtsbehörden. Diese verfügen im OWiG-Verfahren über dieselben Rechte und Pflichten wie die Staatsanwaltschaft bei der Verfolgung von Straftaten. Zwar werden einige Befugnisse aus Gründen der Verhältnismäßigkeit wieder abgeschwächt,[2] doch haben die Ermittlungsbefugnisse im Ergebnis durchaus Gewicht.[3] Für den im OWiG-Verfahren tätigen Datenschützer ist es daher wichtig ein Gespür für die mögliche Einleitung eines Bußgeldverfahrens zu entwickeln. Hierfür genügt bereits die Möglichkeit

[1] BeckOK DatenschutzR/Brodowski/Nowak BDSG § 41 Rn. 47 mwN.

[2] Z.B. ist die Anordnung von Haft im Ermittlungsverfahren nach § 46 Abs. 3 OWIG ausgeschlossen.

[3] Die Aufsichtsbehörde kann im OWiG-Verfahren z.B. nach § 94 StPO Beweismittel sicherstellen und hierfür auf eine Durchsuchung hinwirken.

des Vorliegens einer Ordnungswidrigkeit, womit die Schwelle für ein Tätigwerden der zuständigen Behörde nicht besonders hoch ist, nicht zuletzt auch deswegen, weil Erkenntnisse aus dem Verwaltungsverfahren für die Bejahung eines Anfangsverdachts herangezogen werden können. Sollte der Verantwortliche im Verwaltungsverfahren nach Art. 58 DSGVO mit Fragen konfrontiert werden, deren Beantwortung ihn selbst oder Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzt, besteht die Möglichkeit die Auskunft auf diese Fragen zu verweigern. In der Praxis des Unternehmensstrafrechts ist die Ausübung dieses Rechts ein verbreitetes Verteidigungsmittel.[4] Im Datenschutzrecht mag dies bisher selten genutzt werden, doch muss der Datenschutzverteidiger diese Möglichkeit kennen, um seinen Mandanten in bestimmten Konstellationen vor einer Selbstbelastung schützen zu können. Aus der hohen Anzahl von Verpflichtungen in der DSGVO folgt zwangsläufig, dass ein Auskunftsverweigerungsrecht in vielen Fällen begründbar sein wird.[5] Voraussetzung ist hier dann nur, dass der Verantwortliche sich ausdrücklich auf dieses Recht berufen muss.

C. Das Datenschutzstrafrecht: „Jedermann" kann sich strafbar machen

Im Datenschutzsanktionenrecht muss der Datenschützer das Haftungsregime der bußgeldbewehrten Pflichten der DSGVO und des Strafrechts unterscheiden, weil die Adressaten nicht immer dieselben sind. Für die DSGVO gilt, dass das Bußgeld sich nach § 83 Abs. 3 DSGVO an den Verantwortlichen oder den Auftragsverarbeiter richtet. Im Strafrecht liegen die Dinge anders. Nicht ohne Grund wird im Rahmen des neuen Datenschutzstrafrechts von „Bußgeldrisiken für Unternehmen nach der DSGVO und Strafbarkeitsrisiken für Individualpersonen nach dem BDSG" gesprochen.[6] Im Unternehmensstrafrecht kommt es häufig vor, dass zeitgleich Verstöße im Raum stehen, die sowohl das Unternehmen als auch Individualpersonen betreffen. In Deutschland gilt unverändert, dass die strafrechtliche Haftung von Unternehmen nur vermittelt über die Strafbarkeit der handelnden Personen entstehen kann.[7] Damit besteht zwischen dem Haftungsregime der DSGVO und dem Strafrecht ein fundamentaler Unterschied: Während in der DSGVO regelmäßig das Unternehmen für den Verstoß einzustehen hat, haftet im Strafrecht zunächst die handelnde Person. Besonders gravierend zeigt sich dieser Unterschied, wenn hinsichtlich eines Datenverarbeitungsvorgangs ein strafrechtliches Ermittlungsverfahren wegen § 42 BDSG eingeleitet wird. Nach § 42 BDSG kann (vereinfacht) jede unbefugte Datenverarbeitung eine Verletzung darstellen, wenn es sich um nicht allgemein zugängliche personenbezogene Daten handelt und die Daten auf eine bestimmte Art und Weise oder mit einer bestimmten Absicht verarbeitet werden. Der Anwendungsbereich des § 42 BDSG umfasst prinzipiell jeden Datenverarbeitungsvorgang, wenngleich der Anwendungsbereich im Gegensatz zu DSGVO auf nicht allgemeine öffentlich zugängliche Daten beschränkt ist. Darüber hinaus ist zu berücksichtigen, dass die Straftat nur auf Antrag der betroffenen Person, des Verantwortlichen oder der Aufsichtsbehörde verfolgt wird.[8] Umstritten ist, ob es sich bei § 42 BDSG um ein sogenanntes „Jedermannsdelikt" oder ein „Sonderdelikt" handelt. Dabei geht es im Ergebnis um die Frage, wer als (Haupt-)Täter anzusehen ist. Im Ergebnis sprechen die besseren Argumente dafür,

[4] Über die taktischen Vor- und Nachteile vgl. Klaas/Wybitul/Momsen, Datenschutzsanktionenrecht, § 5, im Erscheinen.

[5] Auernhammer, DSGVO/BDSG, 7. Aufl., § 40 Rn. 32.

[6] So der Titel bei Ihwas, NZWiSt 2021, 289.

[7] Zum Ganzen Rotsch, Criminal Compliance, 1. Teil: Grundlagen § 2 Grundfragen der Criminal Compliance Rn. 1.

[8] § 42 Abs. 3 BDSG.

Ratisbona Compliance

DAS HINSCHG IST DA!

Seit 2. Juli gilt für Unternehmen ab 250 Mitarbeitern das Hinweisgeberschutzgesetz. Ab 17. Dezember 2023 müssen auch Unternehmen ab 50 Mitarbeitern das 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 das Thema Hinweisgeberschutz umsetzen können.

FRAGEN SIE NACH UNSEREN RESELLER-KONDITIONEN

Tel. +49 941 2060384-1

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

dass sich die Strafvorschrift primär an den Verantwortlichen im Sinne der DSGVO richtet.[9] Gleichwohl heißt das nicht, dass Mitarbeiter des Verantwortlichen (des Unternehmens) deswegen von der Strafbarkeit per se ausgeschlossen sind. Denkbar bleibt in diesen Konstellationen nämlich immer noch die Beihilfe zu einer entsprechenden Tat. Wenn der Geschäftsführer zum Beispiel entscheidet nicht allgemein zugängliche Daten zu kaufen, um sie dann für eine Werbeaktion zu nutzen, besteht für die an der Umsetzung beteiligten Mitarbeiter immer dann (auch) ein Strafbarkeitsrisiko, wenn ihnen bekannt ist, dass es sich um nicht allgemein zugängliche Daten handelt und diese zur Generierung neuen Umsatzes für das Unternehmen genutzt werden sollen. In diesem Verständnis würde dann jeder an der Werbeaktion beteiligte Mitarbeiter mit einem Strafverfahren wegen Beihilfe konfrontiert werden können. Überschreiten Mitarbeiter die ihnen eingeräumten Befugnisse in Form eines Mitarbeiterexzesses, sind diese datenschutzrechtlich als Verantwortliche einzustufen,[10] mit der Folge, dass sie sich selbst nach § 42 BDSG strafbar machen (können).

D. Sonderstrafrecht des Datenschutzbeauftragten

Neben der Strafbarkeitsvorschrift des § 42 BDSG gibt es noch weitere Vorschriften, die der Datenschützer kennen muss. Für den Datenschutzbeauftragten betrifft dies zwei spezielle Fallkonstellation. Zum einen wird diskutiert, ob sich der Datenschutzbeauftragte analog zum Compliance Officer durch Unterlassen strafbar machen kann. Auf Grundlage der BGH-Rechtsprechung[11] kommt der Datenschutzbeauftragte als Garant dann in Betracht, wenn die Pflicht zur Aufdeckung von Verstößen und die Pflicht derartige Verstöße künftig zu verhindern oder gar zu unterbinden, auf den Beauftragten als Pflicht des Unternehmens übertragen (delegiert) worden ist. Auf Grundlage dieser Rechtsprechung wird eine vergleichbare Garantenstellung für den Datenschutzbeauftragten im Ergebnis abzulehnen sein. Nach der gesetzlichen Aufgabenbeschreibung in Art. 39 DSGVO hat er die Pflicht Kontrollen durchzuführen, nicht aber die Pflicht Verstöße gegen das Datenschutzrecht zu verhindern oder zu unterbinden. Das bleibt Aufgabe des Verantwortlichen, der anders als der Datenschutzbeauftragte per Definition über die Mittel und Zwecke der Datenverarbeitungen entscheidet. Dies wird man aber nur für den Datenschutzbeauftragten so beurteilen können. Andere Datenschutzfunktionen des Verantwortlichen[12] können durchaus als Garanten in Betracht kommen. Ungeachtet der Rechtsprechung des BGH muss der Datenschutzbeauftragte, der seine Tätigkeit bei Geheimnisträgern ausübt, im Blick behalten, dass speziell er sich durch aktives Tun strafbar machen kann. Dies gilt ganz ausdrücklich gemäß § 203 Abs. 4 S. 1 StGB bei Geheimnisträgern nach § 203 Abs. 1 und Abs. 2 StGB.

E. Vorsicht Falle: Ein Verfahren kann zu einem anderen führen und umgekehrt

Von Datenschützern wird oft vorgebracht, dass sie selten mit strafrechtlichen Verfahren konfrontiert sind. Im Zentrum des Datenschutzsanktionenrechts steht die Verteidigung von potenziellen Bußgeldern gegen Verstöße gegen die DSGVO. Dabei wird allerdings übersehen, dass materiellrechtlich sehr schnell Risiken aus beiden Rechtsgebieten im Raum stehen können. Das ergibt sich schlichtweg aus den typischen Sachverhalten. So wird regelmäßig bei einem Verstoß nach Art. 32 DSGVO auch an entsprechende Straftatbestände nach § 202a, § 303a oder § 303b StGB zu denken sein. In Konstellationen, in denen sowohl ein Bußgeldtatbestand als auch ein Straftatbestand verwirklicht sein kann, muss sich der Datenschutzverteidiger mit dem Konkurrenzverhältnis beschäftigen. Nach § 21 Abs. 1 S. 1 OWiG gilt, dass nur das Strafgesetz angewendet wird, wenn eine Handlung gleichzeitig Straftat und Ordnungswidrigkeit verwirklicht. Insofern ist eine Ordnungswidrigkeit zur Straftat immer subsidiär.[13] Allerdings gilt dies nur, wenn es sich bei dem Sachverhalt um denselben Adressaten handelt. Wenn das Bußgeld also – wie in vielen Fällen – das Unternehmen betrifft, führt das Strafverfahren gegen den verantwortlichen Mitarbeiter nicht dazu, dass das Bußgeldverfahren gegen das Unternehmen entfällt. Taktisch wichtiger ist für den Datenschützer insofern, dass ein strafrechtliches Ermittlungsverfahren in ein datenschutzrechtliches Bußgeldverfahren und ein Bußgeldverfahren in ein Strafverfahren münden kann. Nach § 41 Abs. 1 OWiG ist die Aufsichtsbehörde verpflichtet, die Angelegenheit an die Staatsanwaltschaft abzugeben, wenn Anhaltspunkte dafür vorhanden sind, dass die Handlung eine Straftat ist. Sieht die Staatsanwaltschaft von einer Einleitung des Verfahrens wiederum ab, gibt sie die Sache nach § 41 Abs. 2 OWiG an die Verwaltungsbehörde zurück. Wenn zum Beispiel ein Strafantrag anlässlich einer Videoüberwachung des Nachbargebäudes wegen § 201a StGB gestellt wird und die Staatsanwaltschaft das Verfahren mangels hinreichenden Tatverdachts nach § 170 Abs. 2 StPO einstellt, kann im Anschluss daran die Angelegenheit an die Aufsichtsbehörde weitergeleitet werden. Stellt die Staatsan-

[9] Ihwas, NZWiSt 2021, 289.

[10] Ambrock, ZD 2020, 492.

[11] BGH v. 17.07.2009 - 5 StR 394/08 = NJW 2009, 3173.

[12] So z.B. der vielfach in größeren Unternehmen vorhandene Datenschutzkoordinator.

[13] Krenberger/Krumm, Ordnungswidrigkeitengesetz, 7. Aufl. § 21 Rn. 1a.

waltschaft das Verfahren allerdings nach § 153a StPO unter Auflagen ein, kommt eine weitere Verfolgung nicht mehr in Betracht. Vor diesem Hintergrund muss der Datenschutzverteidiger sich immer auch mit den prozessualen Vorschriften im OWiG und in der StPO vertraut machen, um die Auswirkungen der Entscheidungen für das Folgeverfahren richtig einzuschätzen.[14]

F. Verteidigung ist Kampf und beginnt im Kopf

Zu guter Letzt soll noch darauf hingewiesen werden, dass es zwischen Datenschützern und Strafrechtlern auch kulturelle Unterschiede gibt, die es im Fall eines Sanktionenverfahrens zu überbrücken gilt. In den Standardhandbüchern zur Strafverteidigung liest sich dazu oft der folgende Satz: „Strafverteidigung ist Kampf". Für Datenschützer oder auch für Juristen aus regulierten Gebieten gilt dieser Satz für die eigene Expertise regelmäßig nicht ohne Weiteres. Dort würde es wahrscheinlich heißen: „Verhandlung ist Trumpf". Für Datenschützer dürfte das in den meisten Fällen auch die richtige Strategie sein. In der Praxis wird allerdings bisweilen die Doppelfunktion der Aufsichtsbehörden unterschätzt. Diese üben sowohl die Aufsichts- als auch die Verfolgungsfunktionen in einer Behörde aus. Datenschützer müssen daher ebenfalls in der Lage sein in beiden Rollen zu agieren, und daher im richtigen Moment in den Verteidigungsmodus wechseln. Spätestens bei einer Hauptverhandlung sollte ein Kollege aus dem Strafrecht hinzugezogen werden.

Über den Autor

Dr. Eren Basar, CIPP/E
ist Fachanwalt für Strafrecht und Certified Information Privacy Professional (CIPP/E).

▶ strafrecht.de/de/team/dr-eren-basar/

[14] BeckOK OWiG/Sackreuther, 38. Ed. 1.4.2023, OWiG § 21 Rn. 20.

Anzeige

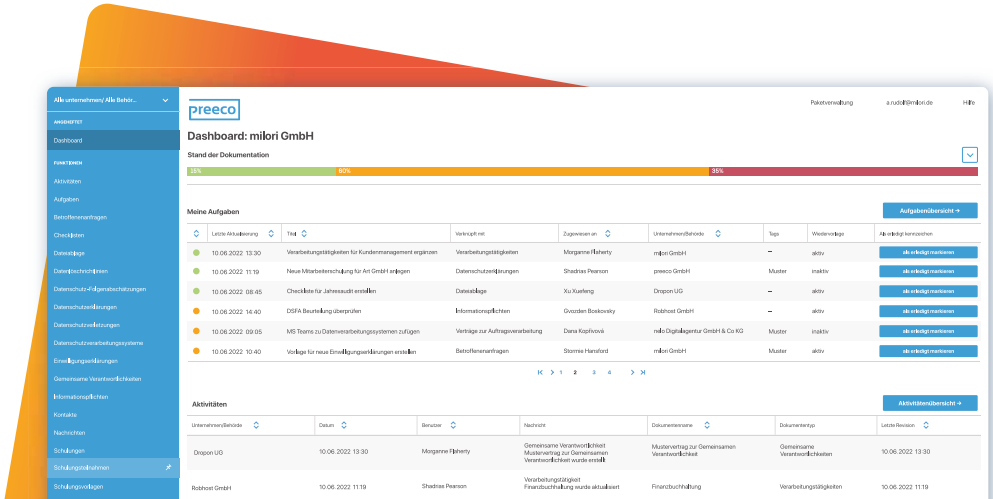
Kostenlos für BvD-Mitglieder: Zwei Stunden Premium Support

preeco

Software für besseren Datenschutz. Schafft Strukturen. Spart Zeit.

Die umfassende Software **preeco | datenschutz** unterstützt Sie als interne und externe Datenschutzbeauftragte sowohl in KMUs, als auch in Konzernen und Behörden.

www.preeco.de/bvd



preeco GmbH
Magirus-Deutz-Straße 14
89077 Ulm
Telefon: +49 731 280 651 0
E-Mail: info@preeco.de
Web: **www.preeco.de**
Amtsgericht Ulm
HRB 737082
Geschäftsführer:
Andreas Hartmann

DR. MATTHIAS LACHENMANN

BESTANDSDATENAUSKUNFT NACH DEM TTDSG

Ein kritischer Einblick und Vergleich mit dem US-amerikanischen Schutzniveau

Die Bestands- und Nutzungsdatenauskunft ermöglicht es Strafverfolgungs- und Sicherheitsbehörden oder Nachrichtendiensten, Informationen über Nutzer:innen von Telemedienanbietern zu erlangen. Dabei können teilweise sehr sensible Daten durch die Behörden erlangt werden, ähnlich zu Gesetzen nach US-Amerikanischem Recht. Durch die §§ 22 – 24 TTDSG werden Telemedienanbieter verpflichtet, bei behördlichen Anfragen bestimmte formale Anforderungen zu prüfen. Der Beitrag beleuchtet die komplexen Prüfpflichten der Telemedienanbieter und gibt Empfehlungen zur Benennung einer verantwortlichen Fachkraft.

Anwendungsbereich der Bestands- und Nutzungsdatenauskunft

Im Rahmen der Bestandsdatenauskunft können Behörden aus den Bereichen Strafverfolgung, Sicherheit und Nachrichtendienste von Anbietern von Telemedien verlangen, Auskunft über Informationen zu ihren Nutzer:innen zu erteilen. Die Auskünfte sollen beispielsweise der Verhinderung von erheblichen Straftaten oder dem Auffinden von vermissten Personen dienen. Möchte eine Sicherheitsbehörde Auskünfte über Daten erhalten, darf der Telemedienanbieter die Daten nur übermitteln, wenn bei ihm die Vorgaben der §§ 22 – 24 TTDSG i. V. m. Art. 6 Abs. 1 S. 1 lit. c, Abs. 3 DSGVO erfüllt sind. Die §§ 22 – 24 TTDSG erfassen alle Anbieter von Telemedien. Konkret trifft das auf jedes Unternehmen zu, das „geschäftsmäßig Telemediendienste erbringt, daran mitwirkt oder den Zugang zur Nutzung daran vermittelt" (§§ 22 Abs. 1 S. 1, 23 Abs. 1 S. 1 und § 24 Abs. 1 S. 1 TTDSG). Darunter fallen beispielsweise Webseiten- und App-Betreiber oder Cloud-Anbieter.[1]

Was ist die Bestandsdatenauskunft?

Bestandsdaten sind Daten zu Kunden:innen, die im Zusammenhang mit dem Abschluss oder der Durchführung von Verträgen stehen. Im Rahmen der Auskunft über Bestandsdaten kann die Polizei einen Onlineshop-Betreiber beispielsweise auffordern, alle zu einer Nutzerin oder einem Nutzer gespeicherten Informationen herauszugeben, beispielsweise Name, IP-Adresse oder Passwörter. Die Vorschriften zur Bestandsdatenauskunft beruhen in ihrer jetzigen Fassung maßgeblich auf der Rechtsprechung des Bundesverfassungsgerichts.[2] Die daraus entwickelten Normen über das Verfahren der Datenübermittlung finden sich in den §§ 22 und 23 TTDSG. Zusätzlich gibt es Vorschriften in den Gesetzen, die das Verfahren bei den Behörden regeln (z. B. im BKA-Gesetz).

Was ist die Nutzungsdatenauskunft?

Bei Nutzungsdaten handelt es sich um Informationen in Zusammenhang mit Nutzung der Telemediendienste. Dazu zählen insbesondere Daten darüber, dass eine betroffene Person Interesse an bestimmten Inhalten hat, wie Aufrufe einer Website zu bestimmten Themen. Die Nutzungsdatenauskunft ist inhaltlich Teil der Bestandsdatenauskunft, jedoch in § 24 TTDSG gesondert geregelt. Solche Auskunftsersuchen stellen gegenüber der Bestandsdatenauskunft tiefergehende Eingriffe in Persönlichkeitsrechte dar und unterliegen daher strengeren gesetzlichen Vorgaben.

Wann dürften Telemedienanbieter Daten herausgeben?

Telemedienanbieter dürfen Daten im Rahmen der §§ 22 – 24 TTDSG nur herausgeben, wenn sie die Anfrage der Behörde auf verschiedene formale Anforderungen überprüft haben. Die Prüfung ist – aufgrund der Vorgaben des Bundesverfassungsgerichts in Form des sog. „Doppeltürmodells" – durchaus komplex. Es ist zu unterscheiden zwischen einerseits der Datenübermittlung durch den Telemedienanbieter („erste Türe") und dem Datenabruf bzw. der Erhebung seitens der behördlichen auskunftsersuchenden Stelle („zweite Türe").[3] Nur wenn die Behörde die Erlaubnis hat, die Daten zu empfangen und zu verarbeiten, darf der Telemedienanbieter die Daten herausgeben. Die Telemedienanbieter müssen allerdings nicht inhaltlich prüfen, ob die materiellen Voraussetzungen der Rechtsgrundlage für die Abfrage von Seiten der Behörde

[1] Lachenmann, in: Gierschmann/Baumgartner, TTDSG, 1. A. 2023, § 22 TTDSG Rn. 9.

[2] BVerfGE 130, 151 (Bestandsdatenauskunft I); BVerfGE 155, 119 (Bestandsdatenauskunft II).

[3] BT-Drs. 19/25294, 53; § 22 Abs. 2 S. 5 TTDSG und BVerfGE 155, 119, 202 (Bestandsdatenauskunft II).

erfüllt sind (z. B., ob ein:e Kunde:in einen Terroranschlag planen könnte). Die Verantwortung für die Zulässigkeit der Auskunft verbleibt bei der um Auskunft ersuchenden Stelle.[4] Allerdings stellt bereits diese formale Prüfung für Telemedienanbieter eine hohe Hürde dar.

Was sollten Telemedienanbieter bei Erhalt eines Auskunftsersuchens tun?

Zwar sehen § 22 Abs. 2 sowie 3 und § 23 Abs. 2 TTDSG vor, dass der Telemedienanbieter lediglich prüft, ob sich eine auskunftsberechtigte Behörde auf eine taugliche Rechtsgrundlage beruft und ihre Ersuchen entsprechend begründet. Jedoch sollten Unternehmen nicht den behördlichen Anfragen vertrauen, sondern eine Prüfung vornehmen, ob die gesetzlichen Vorgaben erfüllt sind. Denn die Herausgabe ist nur rechtmäßig, wenn die Vorgaben von Art. 6 Abs. 1 und 3 DSGVO eingehalten werden.

Insbesondere sollten Unternehmen die folgenden Prüfschritte durchführen:

- Ist in der Anfrage der Behörde eine Rechtsgrundlage benannt, die die konkrete Abfrage der Behörde erlaubt? In der Praxis wird sich z. B. die Polizei oft auf § 100j StPO berufen, der Auskunftsersuchen pauschal zum Zweck der „Ermittlung des Sachverhalts" erlaubt.
- Existiert die Rechtsgrundlage, die die Behörde nannte? Behörden nennen zuweilen nicht mehr existente Normen, z. B. § 14 TMG a. F., da Bundes- und Landesgesetzgeber verschiedene Anpassungen an die neue Rechtslage vorgenommen haben. Eine fehlerhafte Benennung führt dazu, dass das Ersuchen zurückgewiesen werden kann und sollte.
- Erlauben die § 22 – 24 TTDSG die Herausgabe der geforderten Daten durch den Telemedienanbieter auf Basis des von den Behörden genannten Sachverhalts? Diese Prüfung ist meist für Laien kaum sicher zu leisten – hier kann es sinnvoll sein, juristische Beratung einzuholen.
- Erfolgt die Abfrage nur in Bezug auf einen Einzelfall? Die Anfrage darf nicht verschiedene Fälle zusammenfassen.
- Begründet die Behörde, weshalb die Herausgabe der Daten erforderlich ist und was der Zweck des Ersuchens ist?

Wenn sich aus dieser Prüfung ergibt, dass die angefragten Daten herauszugeben sind, ist der Telemedienanbieter verpflichtet, alle unternehmensinternen Quellen zu berücksichtigen und die Daten eigenständig und vollständig zu suchen. Einige Telemedienanbieter veröffentlichen zudem regelmäßig Transparenzberichte. Dadurch können Unternehmen dazu beitragen, rechtswidrige Behördenanfragen offenzulegen und Kund:innen gegenüber demonstrieren, dass der Schutz ihrer Daten streng gewahrt wird.

Nach § 22 Abs. 6 S. 1 TTDSG müssen die abstrakten Vorkehrungen zur Beantwortung der Fragen auf eigene Kosten des Telemedienanbieters getroffen werden. Für die Beantwortung konkreter Anfragen soll laut der Gesetzesbegründung eine geringe Aufwandsentschädigung gezahlt werden. Auch Abrufregelungen aus Fachgesetzen sehen teilweise Entschädigungszahlung vor (bspw. § 40 Abs. 8 BKAG). Im Gesetzestext des TTDSG selbst findet sich eine solche Pflicht aber nicht.[5]

Bestellung einer verantwortlichen Fachkraft

Deutlich wird, dass die Prüfung schwierig und für juristische Laien kaum zu leisten ist. Es empfiehlt sich daher, den Rat von Experten:innen einzuholen. Das können externe Rechtsanwälte:innen sein, die Erfahrung mit der Bestandsdatenauskunft haben oder eine interne Fachkraft, die in dem Gebiet geschult wird. § 22 Abs. 6 S. 2 TTDSG sieht ausdrücklich vor, dass Telemedienanbieter eine verantwortliche Fachkraft bestimmen müssen. Welche Voraussetzungen die Fachkraft mitbringen muss, geht allerdings aus dem TTDSG nicht hervor. Jedenfalls dürfte § 22 Abs. 6 S. 2 TTDSG so zu verstehen sein, dass eine verantwortliche Person bestimmt wird, die eigenhändig (nicht automatisiert, z.B. anhand von Computerprogrammen) die Voraussetzungen der Datenübermittlung überprüft.[6]

Vergleich gesetzlicher Herausgabepflichten in Deutschland und den USA

In EuGH, Urt. v. 16.7.2020 – C-311/18 – „Schrems II" erklärte der Europäische Gerichtshof (EuGH) den EU-US-Privacy-Shield-Beschluss zur Übermittlung von Daten in die USA für ungültig. Grund dafür war, dass aus Sicht des EuGH in den USA kein der Datenschutz-Grundverordnung (DSGVO) und der Europäischen Grundrechtecharta entsprechendes Schutzniveau gewährleistet werde. Ein zentraler Kritikpunkt des Gerichts betraf die niedrigschwelligen Zugriffsmöglichkeiten der US-amerikanischen Sicherheitsbehörden auf die Daten von EU-Bürger:innen. Nachfolgend soll ein Vergleich zwischen den gesetzlichen Bestimmungen der USA und der deutschen Bestandsdatenauskunft gezogen werden.

USA: Foreign Intelligence Surveillance Act und Executive Order 12.333

Abschnitt 702 FISA ermöglicht es, mittels Überwachungsprogrammen Daten über bestimmte Personen zu sammeln.

[4] Lachenmann, in: Gierschmann/Baumgartner, TTDSG, 1. A. 2023, § 22 TTDSG Rn. 10.

[5] Lachenmann, in: Gierschmann/Baumgartner, TTDSG, 1. A. 2023, § 22 TTDSG Rn. 98.

[6] Lachenmann, in: Gierschmann/Baumgartner, TTDSG, 1. A. 2023, § 22 TTDSG Rn. 97.

Diese Sammelerhebungen gewähren den Behörden Zugriff auf umfassende Datenmengen während ihrer Übermittlung. Eine klare und präzise Eingrenzung des Umfangs gibt das Gesetz nicht vor.[7] Im Rahmen der Abfragen der Behörden gibt es keine Aufsicht darüber, ob die Zielpersonen vorschriftsmäßig für die Auslandsaufklärung ausgewählt wurden, nur der gesetzliche Überwachungszweck wir überprüft.[8]

E.O. 12.333 regelt insbesondere die Möglichkeit der NSA, Daten abzufangen und zu speichern, die über die USA übermittelt werden. Da ein Großteil der weltweiten Kommunikation über die Atlantik-Seekabel verläuft, handelt es sich um sehr umfassende Befugnisse. Rechtsschutzmöglichkeiten der Betroffenen bestehen nicht. Welche nachrichtendienstlichen Maßnahmen auf Grundlage der E. O. 12.333 konkret ergriffen werden dürfen, schreibt das Gesetz nicht vor. Für Nicht-US-Personen enthält lediglich die Presidential Policy Directive 28 (P. D. 28) von Präsident Barack Obama Einschränkungen und gibt vor, dass die Überwachungsmaßnahmen „so gezielt wie möglich" sein müssen.

USA: Kein Rechtsschutz gegen die Zugriffe durch Unionsbürger:innen

Nicht-US-Amerikaner:innen können sich gegen als illegal eingestufte Verarbeitungen ihrer personenbezogenen Daten nicht auf den vierten Zusatzartikel zur US-Verfassung berufen, die zentrale Vorschrift gegen illegale Überwachung in den USA. Weitere Rechtsbehelfe gegen Zugriffe auf Basis des FISA und der E. O. 12.333 scheitern praktisch daran, dass Einzelpersonen eine notwendige Klagebefugnis nicht nachweisen können.[9] Tätigkeiten der NSA unterliegen schließlich keiner gerichtlichen Überwachung. Bestimmungen des Privacy Acts erlauben es den Nachrichtendiensten, die Aufzeichnungen über die Überwachungsmaßnahmen dem Gerichtsprozess in bestimmten Fällen vollständig zu entziehen.

Datenzugriffe von Behörden in den USA und Deutschland

Zusammenfassend kann mithin zunächst gesagt werden, dass sowohl in Deutschland als auch in den USA Sicherheitsbehörden und Nachrichtendienste weitreichende Möglichkeiten haben, auf personenbezogene Daten zuzugreifen. Während die §§ 22 – 24 TTDSG nach der Rechtsprechung des Bundesverfassungsgerichts an dem Recht auf informationelle Selbstbestimmung orientiert sind, gelten vergleichbare Garantien für Unionbürger:innen in den USA nicht.

Auch in Deutschland sind die Rechtschutzmöglichkeiten gegen Datenübermittlungen nach dem TTDSG sehr begrenzt. Um gerichtlich gegen Maßnahmen deutscher Sicherheitsdienste vorgehen zu können, muss ebenfalls eine Betroffenheit in eigenen Rechten nachgewiesen werden (Art. 42 Abs. 2 VwGO). Telemedienanbieter müssen gegenüber Betroffenen Stillschweigen wahren (§ 22 Abs. 5 S. 3 TTDSG). Ohne Informationen über die behördlichen Datenabfragen sind die Beweismöglichkeiten der eigenen Betroffenheit und damit im Ergebnis auch der Rechtsschutz stark eingeschränkt.[10]

Deutlich wird, dass auch deutsche Sicherheitsbehörden weitreichende Zugriffsmöglichkeiten auf Nutzer:innendaten haben, deren Anwendung wie bei den US-Behörden selten rechtlich komplett überprüft wird. Die Telemedienanbieter kontrollieren lediglich die formalen Voraussetzungen der behördlichen Datenabfrage, eine Kontrolle des tatsächlichen Vorliegens der Gründe findet – außer in seltenen Fällen der gerichtlichen Überprüfung – nicht statt. Äquivalent dazu

[7] EuGH, C-311/18, 183 (Schrems II)

[8] EuGH, C-311/18, 179, 180, 184 (Schrems II)

[9] Rn. 115 des Durchführungsbeschlusses (EU) 2016/1250 vom 12.07.2016 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes der EU-Kommission

[10] Ausführlich zu der Kritik Lachenmann, in: Gierschmann/Baumgartner, TTDSG, 1

findet auch in US-amerikanischen Behörden keine Aufsicht darüber statt, ob Zielpersonen vorschriftsmäßig für Beschaffung von Auslandsaufklärungsdaten ausgewählt wurden.

Gleichzeitig lässt sich auch die deutsche Bestandsdatenauskunft nicht mit dem Schutzniveau von geltendem Unionsrecht messen. Weder die europäischen Grundrechte noch sonstige Unionsrechtsakte sind auf nationale Regelungen über die Befugnisse der eigenen Nachrichtendienste anwendbar (Art. 51 Abs. 2 EuGRCh und Art. 6 Abs. 1 EUV). Ein Vergleich des europäischen und deutschen Datenschutzrechts in Hinblick auf Bestandsdatenauskunft kann daher nur begrenzt sinnvoll sein.

Jedenfalls ist die Europäische Kritik am VS-Recht nur eingeschränkt gerechtfertigt, da die EU-Länder ähnliche Bestimmungen etabliert haben.

Über den Autor

Dr. Matthias Lachenmann
ist Rechtsanwalt und Partner bei BHO Legal PartGmbB in Köln. Er promovierte zur "Datenübermittlung im Konzern" und ist als Fachautor und Herausgeber des „Formularhandbuch Datenschutzrecht" bekannt.

FAZIT UND EMPFEHLUNGEN

Angesichts der Komplexität und Sensibilität der Thematik ‚Bestandsdatenauskunft' ist von besonderer Bedeutung, dass Telemedienanbieter bei Auskunftsersuchen von Behörden ihren Pflichten nach den §§ 22 – 24 TTDSG nachkommen und Informationen nicht ohne umfassende Prüfung herausgeben. Die Beachtung der Datenschutzbestimmungen und die Gewährleistung eines angemessenen Schutzniveaus für die Nutzer:innen sind entscheidend, um die Balance zwischen Strafverfolgung und dem Schutz der Privatsphäre zu wahren. Der Vergleich mit den viel kritisierten Datenauskunftsbefugnissen US-amerikanischer Behörden zeigt, dass auch deutsche Behörden sehr umfassend auf Daten zugreifen können. Umso wichtiger ist die Rolle der Telemedienanbieter, im Rahmen ihrer Möglichkeiten und mithilfe von Fachkräften, die behördlichen Auskunftsanfragen auf ihre Rechtmäßigkeit zu prüfen. Zudem kann es sinnvoll sein, Transparenzberichte zu veröffentlichen.

Anzeige

DATENVERARBEITUNG IN EINEM DRITTLAND

Wie lässt sich ein Data Transfer Impact Assessment durchführen?

Regina Mühlich, Bernd Schütze

Als Drittland oder auch Drittstaat werden alle Staaten bezeichnet, welche nicht zur Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (EWR) gehören. Werden unter dem Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) personenbezogene Daten in einem Drittland verarbeitet sind gemäß Art. 44 S. 1 DS-GVO zwingend ***alle in Kap. V der DS-GVO enthaltenen Bedingungen zu erfüllen und auch alle anderen Anforderungen der DS-GVO sind einzuhalten.*** *Es ist dabei unerheblich, ob die personenbezogenen Daten von einem innerhalb der EU befindlichen bzw. agierenden Verantwortlichen oder Auftragsverarbeiter einem anderen Verantwortlichen, einem anderen Auftragsverarbeiter oder sonstigen Dritten (wie z. B. einer staatlichen Behörde) in einem Drittland zur Kenntnisnahme oder Verarbeitung bereitgestellt werden.*

Angemessenheitsbeschluss der EU-Kommission

Entsprechend Art. 45 DS-GVO kann die EU-Kommission nach erfolgter Prüfung gemäß Abs. 2

- einem Drittland,
- einem Gebiet in einem Drittland,
- für ein oder mehrere spezifische Sektoren in einem Drittland oder
- für internationale Organisation

ein angemessenes Schutzniveau attestieren. Dies erfolgt über einen sog. Angemessenheitsbeschluss. Dies bedeutet für die Verantwortlichen und Auftragsverarbeiter, dass, abgesehen von der regelhaften Prüfung gemäß den Anforderungen von Art. 28 DS-GVO, keine Prüfung gem. Art. 44 DS-GVO mehr durchgeführt werden muss, da diese Prüfung bereits durch die EU-Kommission erfolgte.

In **allen anderen Fällen muss der Verantwortliche oder der Auftragsverarbeiter die Prüfung der Einhaltung der Vorgaben der DS-GVO durchführen**. Denn selbst wenn ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter (Unterauftragnehmer) in einem Drittland beauftragt, muss dieser weitere Auftragsverarbeiter (Unterauftragnehmer) gem. Art. 28 DS-GVO vom Verantwortlichen genehmigt werden. Dies kann der Verantwortliche entsprechend den Vorgaben von Art. 28 DS-GVO erst nach einer entsprechend erfolgten Prüfung.

Drittland-Verarbeitung und Schrems-II-Urteil

Dies wurde auch noch mal vom Europäischen Gerichtshof in seinem Urteil vom 16. Juli 2020 in der Rechtssache C-311/18[1] („Schrems-II-Urteil") hervorgehoben: Ein Drittland muss „aufgrund seiner innerstaatlichen Rechtsvorschriften oder seiner internationalen Verpflichtungen tatsächlich ein Schutzniveau der Freiheiten und Grundrechte gewährleisten, dass dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist" (Rn. 104 Schrems-II-Urteil). Es wird somit zwar nicht gefordert, dass das Schutzniveau im Drittland identisch zu dem

[1] EuGH, Urt. v. 2020-07-16. AZ. C-311/18 („Schrems-II"). Online, zitiert am 2023-05-15; verfügbar unter https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1

der EU ist, gefordert ist aber ein mindestens gleich hohes bzw. vergleichbares Schutzniveau, sowohl im Hinblick auf die Vorgaben der DS-GVO als auch auf das Schutzniveaus der EU-Grundrechtecharta.

Bei der Beurteilung, ob das Schutzniveau im Drittland dem in der Union durch die DS-GVO im Licht der Charta garantierten Niveau der Sache nach gleichwertig ist, müssen vom Datenexporteur auch **potenziell mögliche Zugriffe durch staatliche** Behörden wie z. B. Geheimdienst oder Ermittlungsbehörden beachtet werden. Die alleinige Möglichkeit eines staatlichen Zugriffes aufgrund der Gesetzeslage im Drittland reicht aus, damit diese staatlichen Zugriffsmöglichkeiten im Drittland vom Datenexporteur bzgl. der Bewertung des Schutzniveaus im Drittland berücksichtigt und bewertet werden müssen (siehe insbesondere Rn. 87, 89, 105 des Urteils).

Der EuGH führt außerdem aus, wie die gesetzliche Anforderung „durchsetzbare Rechte und wirksame Rechtsbehelfe" zu beurteilen ist (insbesondere Rn. 47, 57, 105 und 147): Art. 77 Abs. 1, Art. 78 Abs. 1 und Art. 79 Abs. 1 DS-GVO sind in Verbindung mit Art. 47 der EU-Grundrechtecharta auszulegen. D. h. jede Person muss das Recht haben **einen wirksamen Rechtsbehelf einzulegen** und die Angelegenheit muss von einem unabhängigen, unparteiischen und **zuvor durch Gesetz errichteten Gericht in einem fairen Verfahren, öffentlich** und innerhalb angemessener Frist **verhandelt** werden.

Standarddatenschutzklauseln entsprechend Art. 46 DS-GVO

Die EU-Kommission erließ 2021 Standarddatenschutzklauseln[2], nannte diese jedoch entgegen den Vorgaben der DS-GVO „Standardvertragsklauseln" (engl. „standard contractual clauses", daher häufig durch „SCC" abgekürzt). Basiert eine Verarbeitung personenbezogener Daten auf den von der EU-Kommission veröffentlichten Standarddatenschutzklauseln, so fordert Klausel 14[3], die für alle Module zwingend anzuwenden ist, ausdrücklich ebenfalls eine (bereits durch die DS-GVO vorgegebene) Prüfung der Rechtsvorschriften und Gepflogenheiten im Drittland, die sich auf die Einhaltung der Klauseln auswirken könnten. Diese Bewertung muss dokumentiert erfolgen und ist auf Anfrage der Datenschutzaufsichtsbehörde dieser zur Verfügung zu stellen (Klausel 14 lit. d).

Data Transfer Impact Assessment

Die Beurteilung, ob diese Vorgaben erfüllt sind oder nicht, wird häufig als „Data Transfer Impact Assessment" (DTIA) oder „Transfer Impact Assessment" (TIA) bezeichnet. Es gibt

[2] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates. Online, zitiert am 2023-05-15; verfügbar unter https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX:32021D0914.

[3] Bei der Interpretation von Klausel 14 sollten insbesondere auch ErwGr. 18, 19, 20 und 21 der Standarddatenschutzklauseln mitberücksichtigt werden

keine gesetzliche Anforderung, wie eine TIA durchzuführen und zu dokumentieren ist. Auch seitens der Datenschutzaufsichtsbehörden finden sich zwar allgemeine Hinweise, aber keine Vorlage zur Durchführung.[4]

Neben administrativen Angaben ist in der TIA die geplante Verarbeitung systematisch zu beschreiben. Es ist außerdem begründet darzulegen, warum die Verarbeitung in einem Drittland erforderlich ist und eine, gegebenenfalls auch teurere, Verarbeitung innerhalb der EU/EWR nicht möglich ist.

Art. 44 DS-GVO verlangt, dass alle Anforderungen der DS-GVO einzuhalten sind. Somit insbesondere auch die in Art. 32 DS-GVO geforderte risikobasierte Betrachtung hinsichtlich der technisch-organisatorischen Schutzmaßnahmen. Somit ist auch das Risiko, welches für die betroffene Person aus einer Drittlandverarbeitung erwachsen könnte, zu bewerten und zu dokumentieren.

Entsprechend dem Schrems-II-Urteil hat die TIA auch eine Beurteilung der Rechtslage im Drittland zu beinhalten, das heißt, die Bewertung, ob das im Drittland vorhandene Schutzniveau dem in der EU vorhandenen Schutzniveau gleichwertig ist und ob betroffene Personen durchsetzbare Rechte und wirksame Rechtsbehelfe besitzen, welchen den Vorgaben der DS-GVO wie auch der EU-Grundrechtecharta genügen.

Gemäß dem Schrems-II-Urteil gehört zu dieser Beurteilung der Gesetze im Drittland auch die Bewertung der Möglichkeit(en) von staatlichen Zugriffen, wenn eine Verarbeitung in einem Drittland erfolgen soll. Entsprechend dem Urteil des EuGH reicht die Möglichkeit eines staatlichen Zugriffs aus, damit diese Möglichkeit berücksichtigt werden muss.

Praxishilfe zur TIA

Um den Umgang mit der für eine Verarbeitung im Drittland erforderlichen Bewertung zu erleichtern, haben der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. und die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS) eine 20-seitige Praxishilfe erarbeitet. In der Handreichung wird sowohl der rechtliche Hintergrund als auch das Vorgehen bei der Durchführung einer TIA beschrieben. Ergänzend wird anhand einer Excel-Tabelle gezeigt, wie man eine TIA durchführen kann.

Die Praxishilfe wie auch die Excel-Tabelle sind unter einer freien Lizenz im Internet sowohl auf der Seite der GMDS Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

▶ gesundheitsdatenschutz.org/html/tia.php

als auch im Mitgliederbereich des BvD e.V.

▶ bvdnet.de/wp-content/uploads/2023/04/Data-Transfer-Impact-Assessment_Einfuehrung.pdf

abrufbar.

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.

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. Mitglied im Ausschuss Recht & Politik sowie Leiterin des Committee Law & Politics des EFDPO.

▶ AdOrgaSolutions.de

[4] Lediglich die nicht mehr zu den europäischen Aufsichtsbehörden gehörende ICO veröffentlichte 2018 eine Vorlage für eine DPIA, welche aber nicht alle Anforderungen aus dem Schrems-II-Urteil berücksichtigt: ICO (2018) sample DPIA template. Online, zitiert am 2023-05-15; verfügbar unter https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx

Anzeige

DIE Community für den Service-Nachwuchs.

Networken, lernen und sich entwickeln für Nachwuchs-Führungskräfte – mit dem Young Professionals@KVD-Programm.

Infos anfordern per Mail an **gs@kvd.de** oder unter **www.service-verband.de/young-professionals-kvd**

KVD Der Service-Verband

KIRSTIN VEDDER, CARSTEN LAUMANN

SCHRITT FÜR SCHRITT ZUM DATENSCHUTZ

Auch fünf Jahre nach Einführung der DSGVO tun sich gerade kleine Unternehmen noch schwer damit die Anforderungen umzusetzen. Mit der Website „Datenschutz für Kleinunternehmen" macht die Stiftung Datenschutz ein Angebot für Datenschutzverantwortliche – auch dann, wenn im Unternehmen keine Benennungspflicht besteht.

Die magische Zahl lautet 20. Denn Unternehmen müssen einen Datenschutzbeauftragten bestellen, sobald 20 Beschäftigte regelmäßig in die Verarbeitung von personenbezogenen Daten involviert sind. Das war auch schon die einzige Erleichterung, die der Gesetzgeber mit Inkrafttreten des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes am 26. November 2019 den „kleinen Unternehmen und Vereinen" zugestanden hat. Denn die Erweiterung von ursprünglich 10 auf 20 Personen geht nicht mit sonstigen Erleichterungen zur Umsetzung von Datenschutzanforderungen einher.

Wie ist das Angebot entstanden?

Dass die Unternehmen ohne Benennungspflicht dennoch den Datenschutz einhalten müssen, steht außer Frage. Das Thema bleibt also für kleine Unternehmen von großer Bedeutung, stellt jedoch auch nach fünf Jahren DSGVO oft noch eine Herausforderung dar. Genau hier setzt die Stiftung Datenschutz an. Mit „Datenschutz für Kleinunternehmen" haben wir ein neues Informationsangebot entwickelt:

▶ ds-kleinunternehmen.de

> *„Unser Ziel ist es Kleinunternehmen zu ermutigen den Datenschutz endlich anzugehen und unvoreingenommen loszulegen. Wir möchten zeigen, dass der Schutz personenbezogener Daten nicht nur eine rechtliche Verpflichtung ist, sondern auch eine spannende Reise voller Chancen und Möglichkeiten sein kann. Unternehmen, die jetzt den ersten Schritt machen, können Vertrauen bei ihren Kunden aufbauen, Prozesse verbessern und ihre Wettbewerbsfähigkeit für die Zukunft stärken. Datenschutz zu verstehen trägt auch dazu bei die Scheu vor anstehenden und notwendigen Digitalisierungsprozessen im Unternehmen abzubauen."*
>
> Frederick Richter, Vorstand Stiftung Datenschutz

Das Angebot „Datenschutz für Kleinunternehmen" entspringt der festen Überzeugung, dass der Datenschutz bei Kleinunternehmen zwar angekommen ist, sich das WIE und WAS aber noch nicht so recht für Verantwortliche erschließt. Noch immer bestehen Missverständnisse zwischen den Erwartungen von Verantwortlichen und den Aufgaben von Datenschutzbeauftragten. Manche Erwartungshaltung lässt sich mit folgendem Ausruf zusammenfassen: „Du hast eine Datenschutzbeauftragte? Toll, dann hast du ja jemanden, die den Datenschutz für euch übernimmt!" So macht sich schnell Ernüchterung breit, wenn Unternehmen feststellen, dass sie stattdessen den Großteil der Aufgaben selbst erfüllen müssen. Mit unserem Angebot setzen wir deshalb vor allem auf eine dauerhafte Motivation.

iStock.com/kzenon

Die Entwicklung von der Planung bis zur Veröffentlichung der Website verlief nicht immer ohne Diskussion. Mit Carsten Laumann und Kirstin Vedder trafen zwei unterschiedliche Herangehensweisen aufeinander. Während der Rechtsanwalt Carsten Laumann gerne die Haftungsrisiken für Unternehmen anbringt, möchte die Pragmatikerin Kirstin Vedder lieber überhaupt zum Starten und Dranbleiben motivieren. So zitiert der Jurist aus dem Gesetzestext, aber die Datenschutzberaterin schmeißt alle Paragraphen, Artikel und juristischen Wortspielereien für eine bessere Lesbarkeit wieder raus. So entstand ein Mix, der für Datenschutz-Laien und Datenschutz-Verantwortliche gleichermaßen funktioniert.

An wen richtet sich das Angebot?

„Datenschutz für Kleinunternehmen" richtet sich speziell an Kleinunternehmen, die mit den Herausforderungen bei der Umsetzung des Datenschutzes konfrontiert sind. Kleinstunternehmen, kleine Unternehmen und Selbstständige jeglicher Branchen – egal, ob sie solo oder im Team arbeiten, ob sie einem freien Beruf nachgehen, ob sie eine Neugründung planen oder sich mittendrin befinden – unterliegen oftmals keiner Benennungspflicht und müssen ohne die Unterstützung von Beratungsleistungen den Datenschutz gleichwohl gewährleisten.

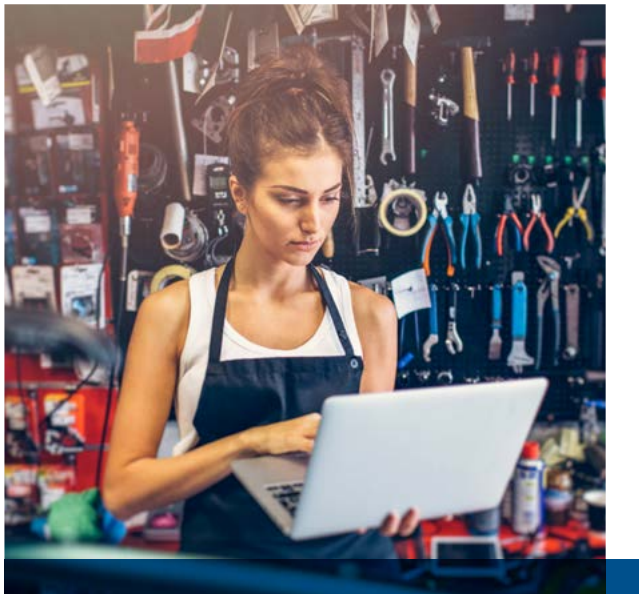
In Handwerksbetrieben, Friseursalons, Haustiertagesstätten oder kleinen Agenturen fehlt es häufig an Fachwissen und Ressourcen, um Risiken zu erkennen und Datenschutzmaßnahmen angemessen umzusetzen. Zudem besteht Unsicherheit darüber, wie man Datenschutzrichtlinien entwickelt und technische und organisatorische Maßnahmen bestimmt, umsetzt und dokumentiert.

Unserer Erfahrung nach empfinden viele Unternehmer:innen, dass im Geschäftsalltag einfach die Zeit fehlt sich kontinuierlich mit dem Thema Datenschutz auseinanderzusetzen. Wer kennt es nicht? Irgendwie gibt es immer wieder gerade Wichtigeres zu erledigen. Wir können auch nachvollziehen, dass sich die Motivation, den Datenschutz anzupacken, in Grenzen hält angesichts der vielen Aufgaben und Pflichten, die es in Sachen DSGVO wahrzunehmen gilt. Vier Hauptprobleme konnten wir in unserer Arbeit mit Kleinunternehmen definieren:

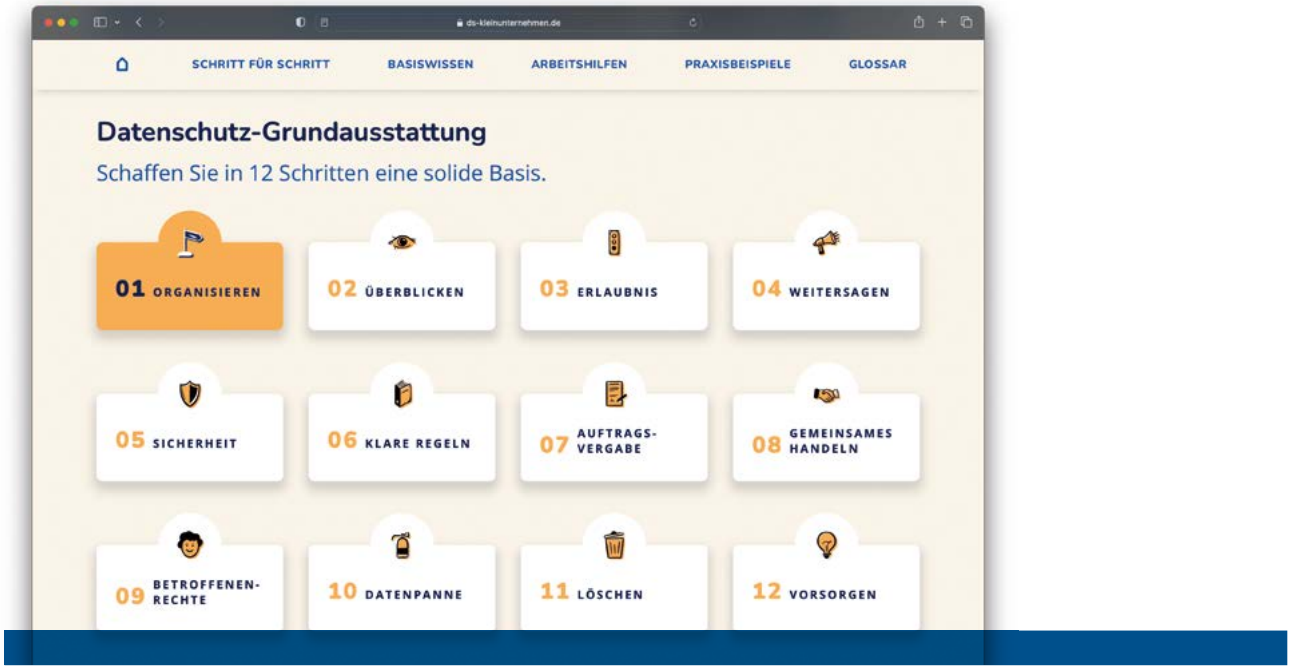
- **Mangelndes Fachwissen und Ressourcen:** Kleinunternehmen verfügen oft nicht über ausreichendes Know-how im Bereich Datenschutz und haben begrenzte Ressourcen, um entsprechendes Fachwissen und Unterstützung einzukaufen.
- **Implementierung technischer und organisatorischer Maßnahmen:** Technische und organisatorischen Maßnahmen umzusetzen, um Datensicherheit zu gewährleisten, kann für Kleinunternehmen eine Herausforderung darstellen. Es fehlt oft an spezifischen IT-Kenntnissen und Ressourcen, um zum Beispiel Schutzklassen zu definieren und geeignete Schutzmaßnahmen zu bestimmen und zu installieren.
- **Unsicherheit bei der Dokumentation und Erstellung von Vorgaben gegenüber den Beschäftigten:** Besonders Selbstständige und kleine Unternehmen sind von einem familiären Umgang geprägt. Mit der akribischen Dokumentation und Festlegung von Pflichten durch Datenschutzrichtlinien sind sie selten vertraut und erleben dies als bürokratische Gängelung. Wie Datenschutzrichtlinien mehr Klarheit und damit Sicherheit im Umgang mit personenbezogenen Daten im Unternehmen auf Dauer fördern können, ist selten bekannt. Fehlen jedoch entsprechende Vorgaben, führt dies wiederum zu erhöhten Risiken in diesen Unternehmen.
- **Zeitmangel und mangelnde Motivation:** Kleinunternehmen sind in der Regel durch den operativen Alltag stark eingespannt. Sich mit dem Datenschutz auseinanderzusetzen rückt daher in der Aufgabenliste nach hinten. Zudem fehlt es manchmal an Motivation sich kontinuierlich um das Thema zu kümmern, weil selten fachlicher Austausch zum Thema innerhalb des Unternehmens stattfindet und die meisten ohnehin beim Thema Datenschutz dankend abwinken.

Mit dem Angebot „Datenschutz für Kleinunternehmen" zielen wir darauf ab typische Probleme der Zielgruppe anzugehen und Unterstützung anzubieten. Es ermöglicht Kleinunternehmen den Einstieg in den Datenschutz zu finden und den Schutz personenbezogener Daten nachhaltig zu gewährleisten. Schritt für Schritt können sich alle, die das Angebot nutzen, eine Datenschutz-Grundausstattung erarbeiten. Praktische Hilfsmittel unterstützen sie dabei die richtigen Fragen zum Datenschutz und zur IT zu stellen. Dies kommt letztendlich auch allen Datenschutzbeauftragten und -beratungen sowie den IT-Verantwortlichen zugute. Die Unternehmen werden besser in der Lage sein zu erkennen, wann sie Hilfe benötigen, und können ihre Erwartungen an die Fachdienstleistungen konkret adressieren.

Die Zusammenarbeit mit externen Datenschutzberatungen oder IT-Dienstleistern ist und bleibt wichtig und spielt eine entscheidende Rolle dabei datenschutzrechtliche Verpflichtungen zu erfüllen. „Datenschutz für Kleinunternehmen" soll deren Dienstleistungen nicht ersetzen, sondern erleichtern und ergänzen.



iStock.com/filadendron



In 12 Schritten gelangen Interessierte zu einer soliden Datenschutz-Grundausstattung.

Wie ist das Angebot aufgebaut?

Das Webangebot „Datenschutz für Kleinunternehmen" ist in verschiedene Bereiche unterteilt, um den Unternehmen ein strukturiertes Vorgehen zu ermöglichen und stets wieder zum roten Faden zurückzufinden. Eine unkomplizierte Sprache und ein pragmatischer Best-Practice-Ansatz bestimmen unser Informationsangebot. Juristische Begriffe haben wir möglichst vermieden und die DSGVO in umsetzbare Teilschritte gegliedert. Wenn ein Themenfeld ein anderes sinnvoll ergänzt, geben wir dazu einen kleinen Hinweis.

Schritt-für-Schritt: Das Herzstück ist unsere Schritt-für-Schritt-Anleitung, die mit einer wiederkehrenden Bildsprache durch die einzelnen Themenfelder leitet.

Hier erhalten die Interessierten eine Anleitung, wie sie den Datenschutz in ihrem Unternehmen im jeweiligen Thema nach und nach umsetzen können. Jeden Schritt erklären wir detailliert und ergänzen ihn mit praktischen Tipps und Empfehlungen. Um die Unternehmen kontinuierlich zu begleiten, werden wir ein Jahr lang jeden Kalendermonat einen der zwölf Schritte hervorheben. Über einen eigens eingerichteten E-Mail-Verteiler, zu dem man sich auf der Website anmelden kann, werden wir zum Dranbleiben motivieren. Somit entlasten wir von dem Druck, sich um alles gleichzeitig kümmern zu müssen. Hauptsache, es geht los! Deshalb steht die Schritt-für-Schritt-Anleitung auch an erster Stelle der Navigation. Wer den Schritten noch nicht zu folgen vermag, kann zur entsprechenden Stelle im Basiswissen wechseln.

Basiswissen: In diesem Bereich finden die Interessierten grundlegende Informationen zum Datenschutz. Wir erläutern die rechtlichen Rahmenbedingungen, erklären Datenschutzprinzipien und definieren grundlegende Begriffe von Auftragsverarbeitung bis Zweckbindung. Häufig gestellte Fragen vervollständigen diese Rubrik: Was sind überhaupt personenbezogene Daten, die verarbeitet werden? Was hat es mit den Grundsätzen einer Verarbeitung auf sich? Und warum ist ein Verzeichnis der Verarbeitungstätigkeiten nötig? Das dürften die Fragen sein, mit denen sich auch gestandene Datenschutzbeauftragte fast täglich konfrontiert sehen.

Arbeitshilfen: Um den Unternehmen die Umsetzung zu erleichtern, hält dieser Bereich praktische Arbeitshilfen bereit, zum Beispiel Vorlagen und Checklisten, die die Nutzer:innen individuell anpassen können. Die Arbeitshilfen werden wir in den kommenden Monaten erweitern und laufend anpassen.

Praxisbeispiele: Datenschutz muss nicht immer neu erfunden werden. Und doch bleibt die Umsetzung für jedes Unternehmen individuell. In den Praxisbeispielen finden Interessierte konkrete Beispiele, die zeigen, wie andere den Datenschutz umgesetzt haben. Diese Praxisbeispiele dienen als Inspirationsquelle und geben wertvolle Einblicke in bewährte Praktiken. Auch die Praxisbeispiele erweitern wir stetig.

Glossar: Da der Datenschutz eine Vielzahl von Fachbegriffen umfasst, erklärt ein Glossar die wichtigsten Begriffe und deren Bedeutung. Dies soll den Unternehmen helfen das Fachvokabular besser zu verstehen.

Zusätzlich zum Webangebot bieten wir Webinare an, in denen Interessierte die Möglichkeit haben ihr Wissen zu vertiefen. Wer sich zum E-Mail-Verteiler anmeldet, erhält regelmäßig

Im Basiswissen informieren sich Interessierte über die wichtigen Aspekte des Datenschutzes.

Informationen zu Neuheiten in unserem Angebot. Außerdem dienen die E-Mails als Motivation kontinuierlich am Datenschutz zu arbeiten und dranzubleiben.

Datenschutz steht nicht still

Das Angebot „Datenschutz für Kleinunternehmen" befindet sich in stetiger Weiterentwicklung, um den sich wandelnden Anforderungen im Bereich Datenschutz gerecht zu werden. Neue Inhalte sowie Werkzeuge, die den Unternehmen helfen den Datenschutz effektiv umzusetzen, sind bereits in Planung. So befindet sich ein Generator für Datenschutzhinweise in der Entwicklung. Nicht nur die gesetzlichen Anpassungen, sondern vor allem das Feedback und die Bedürfnisse der Zielgruppe sollen sich in der Weiterentwicklung niederschlagen.

Datenschutz kann eine Herausforderung sein – insbesondere für Kleinunternehmen, die mit begrenzten Ressourcen an das Thema herangehen. Deshalb freuen wir uns dieses neue und niedrigschwellige Angebot zum Datenschutz kostenfrei anbieten zu können. Wir wollen damit einen Beitrag leisten, diese Lücke so gut es geht zu schließen. Die Stiftung Datenschutz ist fest davon überzeugt, dass Kleinunternehmen mit der richtigen Unterstützung und Motivation in der Lage sind den Datenschutz erfolgreich umzusetzen.

Über die Autoren

Kirstin Vedder
ist zertifizierte Beraterin für Datenschutz und Datenschutz-Auditorin und beschäftigt sich seit 2017 damit den Datenschutz in Organisationen zu verbessern. Ihr Interessenschwerpunkt ist die Implementierung einer Datenschutz-Organisationsstruktur mit geregelten Verantwortlichkeiten und Richtlinien. Ihre pragmatische Sichtweise basiert auf eigenen Erfahrungen in langjähriger Selbständigkeit und in der Datenschutz-Beratung verschiedener Organisationen.

Carsten Laumann
verfügt über langjährige Erfahrung in Theorie und Praxis des Datenschutzrechts, die er als niedergelassener Rechtsanwalt erworben hat. Als Referent für Datenschutzrecht bei der Stiftung Datenschutz bearbeitet er den Schwerpunkt „Datenschutz für Kleinunternehmen" und entwickelt Konzepte und Arbeitshilfen, die kleineren Betrieben, Selbstständigen und Freiberuflern die Umsetzung des Datenschutzes erleichtern sollen.

▶ ds-kleinunternehmen.de

Datenschutz für Kleinunternehmen

Ein Angebot der STIFTUNG DATENSCHUTZ

PETRA MILOSCHEWITSCHOVA, JIRI MNUK, MICHAL NULIÇEK

INTERSECTIONS BETWEEN THE DATA ACT AND GDPR

These are the Issues, Risks and Measures Data Protection Officers Need to Be Aware of

1. Introduction

In recent years, technological advances have accelerated at an unprecedented pace,[1] leading to the emergence of new technologies, inventions and processes on the market that were unforeseen by current legislation. For example, the potential for leveraging data for economic growth, innovation, and societal progress has deepened profoundly, resulting in multiple changes to countless facets of human life. Hand in hand with these developments, the underlying regulatory landscape has also evolved to keep pace with today's dynamic markets.

To tackle these issues, the European Commission has introduced "European strategies"[2] as part of its new priority of "A Europe fit for the digital age",[3] which outlines the EU's goals for forthcoming years. Accordingly, the Commission has set out several objectives in various fields, including data handling and digital services in particular.[4]

This article focuses mainly on the Data Act[5] (**DA**), which forms part of the Commission's broader data strategy. The DA overlaps with several legal areas and poses various legal challenges that Data Protection Officers and lawyers are likely to face. The aim of this article is to articulate those challenges and, to that end, it sets out the broader context surrounding the Commission's data strategy in part 2, presents the selected challenges introduced by the DA (incl. with respect to data, competition law and trade secrets) in part 3, and ends with a brief conclusion in part 4.

2. European Data Strategy

The Commission has sought to reconcile the current incoherence and decentralization of data across different sectors through the creation of so-called "data spaces".[6] Data spaces are envisioned as large, EU-wide databases of specific types of data which can be used by certain subjects, thereby reducing the time and cost required to access such data.

To facilitate the free and comprehensive flow of data within the EU, the Commission has come up with legislative initiatives aimed at establishing fundamental rules for the management of valuable data. This is what is now known as the European data strategy. This set of related regulations and directives includes among others those outlined below.

First, to fulfil its aim of making the online world safer and more transparent and making the online market fairer and more competitive, the Commission proposed the Digital Services Act[7] (**DSA**) and the Digital Markets Act[8] (**DMA**). Second, to ensure the free flow of data within the European market, the Commission proposed two pieces of legislation, namely the Data Governance Act[9] (**DGA**), which sets basic rules for access to, the transfer of and reusability of data held by the public sector, and the DA[10], which focuses on data within the private sector.

3. Data Act

The primary objective of the DA is to stimulate market competition and provide more control to both businesses and consumers by enabling access to industrial data, which means personal and non-personal data, generated through the use of products or related services (**Data**).[11] The DA introduces new rights and obligations associated with the new positions created within the Data handling and processing value chain. To enhance clarity, this article uses a car manufacturing example throughout to elaborate on these issues.

The entire process starts with a **Manufacturer**,[12] which produces individual car parts or entire cars. A **Data Holder**[13] then has the right and obligation to provide access to the Data to the User or Data Recipient, e.g. an automotive company. The Data Holder may or may not also be the Manufacturer. The **User**[14] is the person who owns, rents, or leases the product

[1] https://ourworldindata.org/technology-long-run, [2] https://commission.europa.eu/strategy-and-policy_en, [3] https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en, [4] Ibidem., [5] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of Data (Data Act), [6] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), [8] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)

[9] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)

[10] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of Data (Data Act)

[11] Recital 17 and Art. 2(1) DA, [12] Art. 1(2) DA, [13] As defined in Art. 2(6) DA., [14] As defined in Art. 2(5) DA

or uses the service, e.g., a car owner or company with fleet cars. The User can be either a natural person or a legal entity (referred to collectively here as an "entity" for the sake of simplicity), e.g. a leasing company, a commercial fleets or another such entity. If the User decides to allow its Data to be disclosed to a third party, e.g., an unauthorised car mechanic, that third party becomes a **Data Recipient.**[15] The Data Recipient is therefore an entity which is different from the User, engaged in activities relating to their trade, to whom the Data Holder makes the Data available.

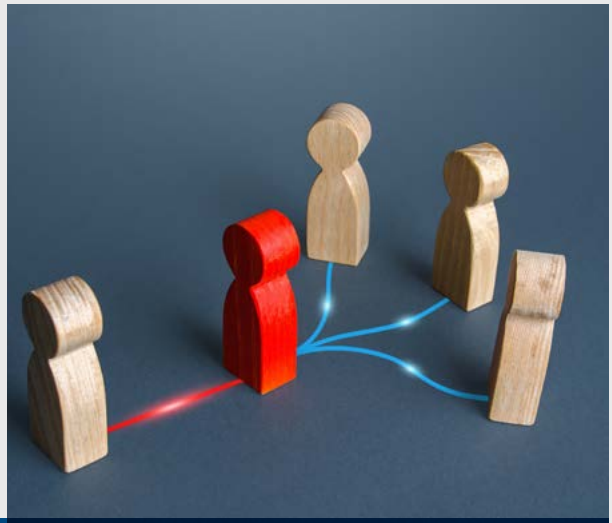
The rules for providing access to Data range from Data format requirements[16] to the possibility of reasonable compensation if the Data is to be made available to someone other than the User.[17] The relevant rules (along with other types of interrelated legislation) are discussed in detail below.

3.1. DPO's Obligations Arising Directly from the Data Act

DPOs and the lawyers (hereinafter collectively referred to as "DPO") are required to assist their respective entities in fulfilling the new obligations arising from the DA. Before starting to fulfil any of these obligations, the DPO must first assess the position in which its respective entity finds itself.

The Manufacturer oversees the designing of a product. The DA imposes an obligation on the Manufacturer to design the product so that the Data generated by the product are easily accessible (**Accessibility by design**)[18] e.g., directly through an interface in the car itself or through a related application,[19] while maintaining a certain level of security.[20] If direct access is impossible, the User must have an option to access Data upon request.[21] On the one hand, whether access is given in a way compliant with the DA[22] must by assessed by the Manufacturer's and Data Holder's DPO. On the other hand, a DPO working with the User or Data Recipient may need to assist in exercising the right to access or in assessing whether the range of Data provided is sufficient for the desired purpose.

As far as relations between Data Holders and Data Recipients are concerned, DPOs may also assist in communication with respect to Data access and related issues. Such communication becomes particularly important when the terms and conditions for data sharing are negotiated between the Data Holder and Data Recipient.[23] In those cases, DPOs must always support their entity throughout the negotiations and assess the final agreement to ensure that it does not contain any non-compliant (discriminatory or other) clauses.[24]



The Data Recipient is prohibited from coercing, deceiving, or manipulating the User in any way in order to gain access to Data or from preventing them from granting access to their Data to other third parties (through contractual terms or otherwise). If access is granted to Data Recipients, they must not use the Data for conduct such as profiling and they are prohibited from disclosing the Data to Gatekeepers or other third parties. In the case of third parties, there is an exception if such disclosure is, unless it is necessary for the provision of a service by to the User.[25]

Public bodies may also request access to Data under specific circumstances.[26] The Data Holder's DPO will be responsible for both evaluating the request (for example, if there is an exceptional need for the Data) and issuing a statement in relation to it. The public body's DPO may be required to assess the request before it is even issued, as well as evaluate the access granted in response to such request.

The new rules established by the DA may negatively impact the confidence of the respective entities' shareholders. To combat this problem, the DPOs of Data Holders, Users and Data Recipients shall assist in increasing management confidence, for example by way of conducting seminars or otherwise informing shareholders about the DA's positive effects.[27]

Finally, DPOs will need to generally ensure overall compliance by their respective entity. This includes not only assessing compliance with the DA itself, but also with rules laid down by other legislation[28], such as data protection and competition laws, as discussed below.

[15] As defined in Art. 2(7) DA., [16] Art. 3(2) DA, [17] Upon disclosing Data to a third party, the Data Holder may ask the Data Recipient for reasonable compensation, as defined in Art. 9(1) of the DA, [18] Recitals 19, 20 and Art. 3(1) of the DA https://www.acea.auto/files/ACEA-position-paper-Proposal-for-a-Data-Act.pdf., [19] Recital 21, 22 and Art. 3(1) of the DA, [20] https://www.acea.auto/files/ACEA-position-paper-Proposal-for-a-Data-Act.pdf, p. 8., [21] Recital 20 and Art. 4 of the DA, [22] Art. 3(1), [23] In particular Art. 8 and 9 DA, [24] Recitals 41,47 and 52-55 and Art. 8, 9 and 13 of the DA., [25] Art. 6 of the DA, [26] Art. 14, 17 and 18 of the DA, [27] https://www.efdpo.eu/dpos-as-facilitators-for-the-successful-implementation-of-the-data-act/., [28] Art. 1(3,4) and 16(1) of the DA

3.2. Data Act and Data Protection

The DA complements the General Data Protection Regulation (GDPR)[29] when it comes to the protection of personal data.[30] This means that if a User or Data Recipient requests access to a dataset containing personal data, the Data Holder must assess whether they are data subjects[31] or whether they have a legal basis for processing such Data[32]. This becomes very problematic when the User and Data Recipient are not natural persons but legal entities (e.g., commercial fleets) and thus not data subjects. If such a company requests Data, the Data Holder will have to decide in which form the Data will be provided (for example as anonymized data), or whether and what legal title such a company has for processing the personal data transferred. It is therefore debatable whether a Data Holder will require, for example, proof of consent from data subjects or whether consent is an appropriate legal title, especially in the case of an indeterminate scope of data subject (for example a customer of a car rental company). In such situations, the DPO will need to advise the Data Holder on how to proceed, how to anonymize the Data or whether to refuse to provide access to the Data.[33]

This also means that if a dataset containing personal data is requested by anyone except for the data subject, the Data Holder shall assess whether there is a need to conduct a data protection impact assessment,[34] whether they and other subjects will be considered joint controllers[35] or whether their connection will constitute another type of relationship.[36] Accordingly, the Data Holder must also assess the manner in which to perform the duties arising from the information obligation towards data subjects and transparency principles in general.[37] These obligations also apply to the DPO of the User or Data Recipient, as they themselves will need to ensure compliance with the GDPR. In addition, all the relevant actors will also need to fulfil all obligations relating to subsequent use and sharing of the Data, which may be derived either from a contract concluded between them and the Data Holder, or directly from data protection legislation. Since the role of the DA in data protection regulation is only supplementary, the disclosure of personal data in response to a request from the User or a third party shall be governed by the rules and principles laid down by the GDPR. This means that upon any disclosure of personal data, the respective entities must comply with both the DA and the GDPR, as well as any other legislation applicable under the given circumstances of each case.

3.3. Data Act and Competition Law

In order to preserve market competition, the DA establishes a set of rules for all entities that may come in contact with Data. The Data Holder which has the Data at its disposal is obligated not to abuse its position by way of, for example, seeking a competitive advantage against a Data Recipient.[38] This also means that neither party may impose any unfair contractual terms when concluding data sharing contracts.[39] Users themselves may use the Data for any lawful purpose, which can also be providing the Data to a competing subject, to receive an aftermarket service.[40] However, the User is also prohibited from using the disclosed Data for the design and/or production of a competing product or service.[41]

Thus, all parties involved will need to assess whether a product developed based on accessed Data has the competitive nature in relation to the product which produced the Data (based on analysing the competitive relationship or the definition of relevant markets), and thus violates this prohibition. Such an analysis will need to use standard competition law tools for defining relevant markets (including by way of the so-called SSNIP test), assessing the substitutability of various new and existing products, and determining the competitive interactions between various products, including the one which has been newly developed. Conducting such an analysis might be a challenging task and the burden might increase even further due to the unavailability of related information which might enable such an analysis.

In any event, the restriction concerning competing product development is rather controversial. On the one hand, such a restriction ensures the protection of the investments and efforts exerted by the Data Holder or Manufacturer and maintains an incentive to innovate and further improve their services. On the other hand, however, access to Data under the DA strives to remedy the persisting issue of data access restrictions (including data retention by larger undertakings, like Big Tech and other strong players in their respective fields). Those restrictions have resulted in market tipping and the inability of other competitors to replicate or effectively compete with such players.

The use of data in competition with the Data Holder or Manufacturer may take various forms and may be reflected not only in the development of competing products (which the DA restricts) but also in the use of Data for ensuring interoperability

[29] 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)

[30] Recitals 7, 24, 30, 31 and Art. 1(3) of the DA, [31] As defined in Art. 4(1) of the GDPR, [32] Art. 6(1) and 9 of the GDPR as cited by Art. 4(5) and 5(6) of the DA, [33] Results from Art. 12(3) of the DA and Art. 15 of GDPR, [34] As defined in Art. 35 of the GDPR. https://www.efdpo.eu/dpos-as-facilitators-for-the-successful-implementation-of-the-data-act/, [35] As defined in Art. 26 of the GDPR, [36] https://www.engage.hoganlovells.com/knowledgeservices/news/data-act-part-2-unfair-terms-in-data-sharing-agreements, [37] Art. 12 and 13 of the GDPR, [38] Recital 29 of the DA, [39] Recital 25 and Art 13 of the DA, [40] Recital 28 of the DA, [41] Art. 4(4) and 6(2e) of the DA

between various categories of different but complementary products (such as in the sphere of the Internet of Things, but also in more traditional sectors). In that area, ex post competition enforcement seems to have failed on a broader scale.[42] Ex ante regulation in various types of EU legislation (such as the DA) thus seems to provide a more flexible self-executing framework with respect to interoperability.

In the above context, DPOs will need to monitor the use of Data to which access has been granted and assess whether any competing products have been or are being developed based on such Data, or whether the Data are used for other purposes such as ensuring interoperability. That will likely pose a challenging task for DPOs for several reasons, including the fact that the actual use of Data may be unclear.

There will also likely be a fine line between the development of a competing product (determined based on a competition analysis) and a follow-up, complementary or interoperable product.[43] Accordingly, DPOs will in various cases need to seek competition and regulatory advice on these issues. The Data Holder, User and Data Recipient themselves also need to fulfil further obligations imposed on them by general EU competition law (and the relevant rules of EU Member States) and must therefore assess whether conduct concerning Data may, regardless of other obligations in the DA or elsewhere, constitute an anticompetitive practice (e.g., by selectively restricting access to some recipients while granting it to others) or an abuse of dominance (for example by refusing access to Data which constitute an essential facility).[44]

3.4. Data Act and Trade Secrets

Consideration must also be given to trade secrets and intellectual property rights when disclosing Data.[45] If the User requests access to Data that contains a trade secret or other confidential information from the Data Holder, it is assumed that the Data Holder will take all the necessary measures required to ensure the confidentiality of such Data, especially since it can only refuse to provide access to the User when specific circumstances are met[46]. Before disclosing Data containing confidential information to a third party, the Data Holder should conclude a data sharing agreement, which should ensure adherence to the measures necessary to preserve confidentiality.[47] The general principle when providing access to confidential data is that the Data Holder cannot be obligated to provide trade secrets as defined in Directive (EU) 2016/943.[48] Therefore, before disclosing any confidential information, Data Holders may (and in some cases must) identify the necessary scope of disclosure to fulfil the principle of data minimization, as well as identify the specific measures necessary to preserve confidentiality. They shall then impose these measures on third parties through contractual terms, or, in the case of User, agree upon which measures should be put into place.

4. Conclusion

The DA is likely to have a significant impact on DPOs, regardless of which entity they assist. The DA is likely to introduce new rights and obligations for which it will be necessary to set up adequate compliance and monitoring processes. The fundamental ideas behind the DA seem promising, but work still needs to be done to align it with the GDPR and other privacy laws, but also to, for instance, better protect intellectual property and trade secrets and clarify the interplay between the DA and general EU competition law. All of this presents an opportunity for growth and advancement of the Commission's strategy. However, multiple questions remain unanswered, thus potentially introducing uncertainties. Going forward (and subject to the final wording of the DA) DPOs will likely need to facilitate cooperation among various teams to gather the necessary insights and appropriately resolve those issues and uncertainties.

Über die Autoren

Michal Nulíček
is a Partner at ROWAN LEGAL specializing in data protection, IT and IP law, as well as competition law, compliance and all areas of regulation.

Jiří Mňuk
is a Partner at ROWAN LEGAL specializing in data protection, IT and IP law, as well as competition law, compliance and all areas of regulation.

Petra Miloschewitschová
a is a Junior Lawyer at ROWAN LEGAL specializing mainly in data protection and privacy regulation. Other areas she focuses on are ICT law, e-commerce and contracts.

[42] See, for example, Nicholas Economides, Ioannis Lianos and Luca Rubini, 'The Quest for Appropriate Remedies in the EC Microsoft Cases: A Comparative Appraisal' in Luca Rubini, Microsoft on Trial (Edward Elgar Publishing 2010), [43] Greaf, I., & Husovec, M. (2022). Seven Things to Improve in the Data Act. Available at SSRN 4051793, p. 2, [44] In particular Art. 101 and 102 of the Treaty on the Functioning of the European Union, [45] Recitals 28 and 66 of the DA, [46] Recital 28, Art. 4(3) of the DA and Podszun, R., & Offergeld, P. (2022). The EU Data Act and the Access to Secondary Markets. Available at SSRN 4256882, p. 42, [47] Art. 5(8) of the DA, [48] Art. 8(6) of the DA and Podszun, R., & Offergeld, P. (2022). The EU Data Act and the Access to Secondary Markets. Available at SSRN 4256882, p. 42

KI UND DATEN-SCHUTZ

Dr. Jan Wacke, Dr. Peter Nägele

Die Bedeutung von Anwendungen mit Künstlicher Intelligenz (KI) nimmt unbestreitbar zu. Seit einiger Zeit können etwa beeindruckende Anwendungen mit KI im Bereich der Textübersetzung und Sprachverbesserung genutzt werden. An Hochschulen werden KI-Assistenten und KI-Tutoren entwickelt, die Studierende beim Lernen unterstützen sollen.[1] In der Medizin sind vielversprechende Anwendungen[2] erkennbar, beispielsweise bei der Krebserkennung und der Entwicklung neuer Antibiotika.[3] Gleichzeitig warnen die Geschäftsführer von OpenAI vor dem Einsatz von KI und fordern, jede weitere Entwicklung Künstlicher Intelligenz, die eine bestimmte Schwelle überschreite, müsse der effektiven Aufsicht durch eine internationale Behörde unterstellt werden. Denn: „Die Systeme, die wir mit Sorge betrachten, haben eine Macht, die der jeder bisher geschaffenen Technologie überlegen ist".[4] Zugleich empfehlen sie einstweilen eine freiwillige Selbstverpflichtung zur Begrenzung der Entwicklung. Allerdings ist der Gesetzgeber hier nicht so langsam, wie oft unterstellt wird. Die Datenschutz-Grundverordnung (DSGVO) hat gerade ihren fünften Geburtstag gefeiert, und die europäische KI-Verordnung wird voraussichtlich noch in diesem Jahr verabschiedet. Die Produkthaftungsrichtlinie wird derzeit überarbeitet und soll künftig auch Softwarehersteller in die Haftung nehmen. Alle Unternehmen, die den europäischen Markt bedienen, müssen sich an die europäischen und nationalen Gesetze halten und können sich nicht nur auf eine freiwillige Selbstverpflichtung berufen. Auch wenn allgemein Verhaltensregeln (Codes of Conduct) und Zertifizierungen zur Einhaltung rechtlicher Rahmenbedingungen einen sinnvollen Beitrag leisten können, weist die gesellschaftliche Wirkung von KI jedoch klar darauf hin, dass es hier eines vorgegebenen Rechtsrahmens bedarf.

Transparenz und Richtigkeit

In Artikel 8 Absatz 2 der Charta der Grundrechte der EU wird ausdrücklich das Auskunfts- und Berichtigungsrecht bei der Verarbeitung personenbezogener Daten normiert. Nur wer weiß, welche die eigene Person betreffenden Daten zu welchem Zweck verarbeitet werden, kann seine Grundrechte wahrnehmen. Transparenz darüber, wie Daten verarbeitet und Ergebnisse erzielt werden, ist notwendig, um gesellschaftlich, individuell und rechtlich entscheiden zu können, ob eine Verarbeitung erwünscht ist oder nicht. Bei KI-gestützten Verarbeitungen können jedoch Unklarheiten über die Funktionsweise bestehen. Wie der EuGH in seinem Urteil zur Verarbeitung von Fluggastdaten feststellt,[5] kann es sich nämlich „angesichts der für die Funktionsweise von Technologien der künstlichen Intelligenz kennzeichnenden mangelnden Nachvollziehbarkeit als unmöglich erweisen

[1] ChatGPT geht an die Uni, FAZ 20.5.23

[2] Artificial intelligence in healthcare and education, M. Dave, N. Patel, British Dental Journal 234 761-764 (2023), https://doi.org/10.1038/s41415-023-5845-2. Der Artikel wurde mit ChatGPT erstellt

[3] Deep learning-guided discovery of an antibiotic targeting Acinetobacter baumannii, G. Liu et al., Nature Chemical Biology (2023), https://doi.org/10.1038/s41589-023-01349-8

[4] KI wirkt atomar, FAZ 25.5.23

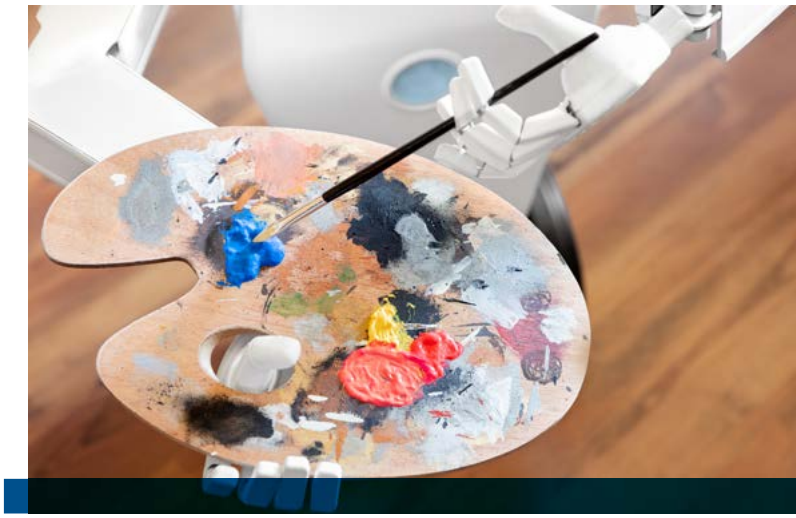
[5] EuGH Urt. v. 21.6.22 – C-817/19 2022 – Rn. 195

den Grund zu erkennen, aus dem ein bestimmtes Programm einen Treffer erzielt hat". Wie sollen sich Bürger_innen rechtsstaatlich gegen einen „Treffer" wehren und Gerichte darüber urteilen können, wenn nicht nachvollziehbar ist, wie ein solcher Treffer zustande kommt?

Ein grundsätzliches Problem – Statistik

Die Art und Weise, wie ein GPT (Generative Pre-trained Transformer) – aber auch andere KI-Verfahren – Ergebnisse erzeugt, ist statistisch bestimmt. Die Antworten werden generiert, indem die wahrscheinlichsten Wörter zu einem Satz zusammengestellt werden. Dabei werden nicht nur Fehlinformationen aus den Trainingsdaten reproduziert, sondern auch neue Fehlinformationen und entsprechende Fehlverweise erzeugt, die diese scheinbar bestätigen.[6] Dies muss für sich genommen nicht besonders problematisch sein. Je nach Kontext, in dem die KI eingesetzt wird, ergeben sich für Bürger_innen in vielen Fällen aus solchen Fehlern keine Konsequenzen. Es gibt jedoch auch Gegenbeispiele mit gravierenden Folgen. Der Kontext, in dem eine KI eingesetzt werden soll, muss daher für KI geeignet sein. Ein Beispiel für einen in diesem Sinne (noch) ungeeigneten Kontext mag der Einsatz von ChatGPT durch einen amerikanischen Anwalt zur Recherche für ein Gerichtsverfahren sein: Die KI soll dabei zur Begründung ihrer Ausführungen auf frei erfundene Gerichtsentscheidungen verwiesen haben – mit der Folge, dass der Anwalt, mutmaßlich nicht zum Vorteil seiner Mandantschaft, nunmehr im Verdacht steht, er habe das Gericht täuschen wollen.[7]

Ein grundsätzliches Problem tritt insbesondere dann auf, wenn wenige Ereignisse in einer großen Datenmenge erkannt werden sollen. Der Satz von Bayes aus der Statistik zeigt, dass es dabei zwangsläufig zu (vielen) falschen „Treffern" kommt.[8] Der Einsatz von KI in Bereichen, in denen potenziell schwerwiegende Eingriffe in die Grundrechte von Bürger_innen vorgenommen werden, ist daher heikel. Beispiele hierfür sind die biometrische Gesichtserkennung zur Identifizierung von Straftätern[9], die KI-gestützte „Klassifizierung" von Fluggastdaten oder die Erkennung von Sozialbetrug.[10] Um dieses Grundproblem zu lösen, muss die Qualität der KI-Ergebnisse deutlich verbessert werden. Nur so kann rechtsstaatlichen Anforderungen einschließlich des Grundsatzes der Verhältnismäßigkeit entsprochen werden.



Bias und Diskriminierung in algorithmischen Systemen

Bias und Diskriminierung finden sich nicht nur in (Trainings-) Daten und Algorithmen. Sie treten in allen Phasen der Produktentwicklung auf.[11] Die Europäische Agentur für Grundrechte hat die inhärente Voreingenommenheit von KI-Modellen untersucht und bestätigt.[12] Einzelne Wörter machten in ihrer Studie einen großen Unterschied: So bewertete eine untersuchte KI die Aussage „Ich bin Christ" als weniger anstößig als die Aussage „Ich bin Muslim". Das stellt die KI-basierte Erkennung von Hassrede und beleidigender Sprache vor ein zentrales Problem. (Struktureller) Bias in den Daten führt zu (struktureller) Diskriminierung. Vermutlich kennt jede Gesellschaft Bias, auch ohne KI. Die Reproduktionsrate von Bias dürfte bei KI aber deutlich größer sein.

[6] https://www.tagesspiegel.de/kunstliche-intelligenz-der-plappernde-papagei-im-netz-9381044.html; https://www.nytimes.com/2023/05/27/nyregion/avianca-airline-lawsuit-chatgpt.html

[7] S. z. B. https://www.zdf.de/nachrichten/digitales/chatgpt-anwalt-klage-gericht-antrag-recherche-scheitern-100.html.

[8] https://de.wikipedia.org/wiki/Satz_von_Bayes

[9] (Pilot)Projekt Biometrische Gesichtserkennung Bahnhof Berlin Südkreuz, u.a. https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=B00C5E4B9341D9F8733EF8508A6D9C46.2_cid324?__blob=publicationFile&v=1

[10] Dazu: The Hague District Court C/09/550982 / HA ZA 18-388, 2020

[11] Denkimpuls Digitale Ethik: Bias in algorithmischen Systemen – Erläuterungen, Beispiele und Thesen, C. Balkow et al., Initiative D21, 2019, u.a. Abbildung 1

[12] Bias in Algorithms – Artificial Intelligence and Discrimination, European Union Agency for Fundamental Rights, 2022, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf

Meinungsbildung, Werbung und Zeit

Der Skandal um Cambridge Analytica[13] zeigt die Möglichkeiten auf mit personenbezogenen Daten psychologische Profile zu erstellen und Bürger_innen gezielt mit (Wahl-)Werbung und Informationen zu versorgen. Diese Art der Beeinflussung ist auch fester Bestandteil, wenn es darum geht Nutzende möglichst lange auf einer Plattform zu halten. Sie wird durch KI-Algorithmen optimiert. Kennen wir die Grammatiken, mit denen solche Aufmerksamkeit erzeugt wird, und wie gehen wir mit ihnen um? Darauf muss es gesellschaftlich tragfähige Antworten geben.

Diskussion um ChatGPT

Datenschutzrechtlich entzündete sich die Diskussion über den Einsatz von KI zuletzt besonders am Dienst ChatGPT von OpenAI: Am 30. März 2023 erließ die italienische Aufsichtsbehörde gegen OpenAI ein einstweiliges Verbot der Verarbeitung personenbezogener Daten von betroffenen Personen in Italien mittels ChatGPT. Wesentliche Gründe waren, dass OpenAI keine Informationen über die Verarbeitung personenbezogener Daten zur Verfügung stelle und eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten zum Zweck des Trainings des Algorithmus nicht erkennbar seien. Außerdem sei die Richtigkeit der verarbeiteten personenbezogenen Daten nicht gewährleistet und es finde keine Altersverifikation zum Schutz Minderjähriger statt.[14] Im April kam es aus der Sicht der italienischen Behörde indes zu relevanten Verbesserungen bei ChatGPT, so dass sie die einstweilige Untersagung beendete: Insbesondere stelle OpenAI nunmehr Datenschutzinformationen bereit, räume betroffenen Personen in Europa – auch nicht den Dienst nutzenden – die Möglichkeit ein, der Verarbeitung von sie betreffender Daten zu Trainingszwecken zu widersprechen und Falschinformationen zu löschen, und habe eine Altersabfrage eingeführt.[15]

Auch deutsche Aufsichtsbehörden haben eine Untersuchung eingeleitet. Die Datenschutzkonferenz hat – mit Mitwirkung des LfDI Baden-Württemberg – einen Fragebogen zur Aufklärung entwickelt. Auf dieser Grundlage hat auch Baden-Württemberg OpenAI zu einer Stellungnahme aufgefordert,[16] um zu erfahren, was genau hinter der von ihr betriebenen Anwendung steckt, und sodann eine datenschutzrechtliche Bewertung vorzunehmen.

Die Fragen, die sich für einen Dienst wie ChatGPT und jeden anderen Dienst stellen, sind allgemein und spiegeln die Anforderungen der DS-GVO wider. Es geht insbesondere darum, wie bei der Verarbeitung personenbezogener Daten die Einhaltung der Grundsätze aus Artikel 5 DS-GVO sichergestellt werden, die der Rechtmäßigkeit, der Zweckbindung, der Datenminimierung und Speicherbegrenzung sowie der Datenrichtigkeit. Zu betrachten sind dabei die Daten, mit denen die Anwendung ursprünglich trainiert wurde, ebenso wie jene Daten, die die Nutzenden über sich selbst und Dritte eingeben, und die personenbezogenen Daten, die ChatGPT selbst erzeugt.

Besonderes Augenmerk gilt dabei Datenkategorien mit besonderem Schutzbedarf und dem Schutz Minderjähriger. Ebenso ist zu untersuchen, wie die Rechte betroffener Personen umgesetzt werden und welche technisch-organisatorischen Maßnahmen zum Datenschutz getroffen wurden. Nicht zuletzt ist auch zu untersuchen, welche Rechtsgrundlagen bzw. Regelungen zur datenschutzrechtlichen Verantwortung greifen, wenn datenschutzrechtlich Verantwortliche den Dienst ChatGPT für ihre Zwecke nutzen wollen.

Auch insoweit gilt allerdings, dass hier jeder datenschutzrechtlich Verantwortliche wird prüfen müssen, ob der Einsatz einer (im Falle von ChatGPT: Foundation-Model-)KI im jeweiligen Kontext zulässig und angemessen ist. Insbesondere wenn KI von staatlichen Akteuren eingesetzt wird, ergeben sich potenziell weitreichende und vielfältige Auswirkungen auf Bürger_innen.

[13] S. dazu z. B. https://www.ardmediathek.de/video/planet-wissen/der-fall-cambridge-analytica/wdr/Y3JpZDovL3dkci5kZS9CZWlocmFnLTY5N2RmYTYwLTA1ZTktNGY0Ni1hZTg1LWQyYmY0Njk1YTNmNw

[14] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847

[15] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9881490

[16] S. https://www.baden-wuerttemberg.datenschutz.de/lfdi-informiert-sich-bei-openai-wie-chatgpt-datenschutzrechtlich-funktioniert

Neue europäische Normen

In unserer Betrachtung müssen wir den Blick noch weiten: Neue europäische Regelungen wurden erlassen oder sind in Arbeit (u.a. KI-Verordnung, Data Governance Act, Digital Services Act, Digital Markets Act, Data Act, European Health Data Space, E-Privacy-Verordnung). Diese werden unterschiedliche Bereiche der Digitalisierung regeln. Die DS-GVO wird in Zukunft stärkere Bezüge zu weiteren europäischen Regelungen haben. Aufgabe insbesondere der Datenschutzbehörden wird es dabei sein das komplexe Zusammenspiel des europäischen Digital- und Datenrechts insgesamt zu überblicken. Ihre Ressourcen und Befugnisse müssen entsprechend dem dadurch neu gewichteten Verantwortungsbereich gestärkt werden.

Über die Autoren

Dr. Jan Wacke
ist leitender Beamter beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW).

Dr. Peter Nägele
ist Technischer Referent in der Stabsstelle für Deutsche und Europäische Zusammenarbeit beim LfDI BW.

[17] Von Menschen und Technik: Von der Apokalypse-Angst zur Euphorie, Tagesspiegel, 23.2.01, https://www.tagesspiegel.de/kultur/von-menschen-und-technik-von-der-apokalypse-angst-zur-euphorie-763861.html

SCHLUSSBETRACHTUNG

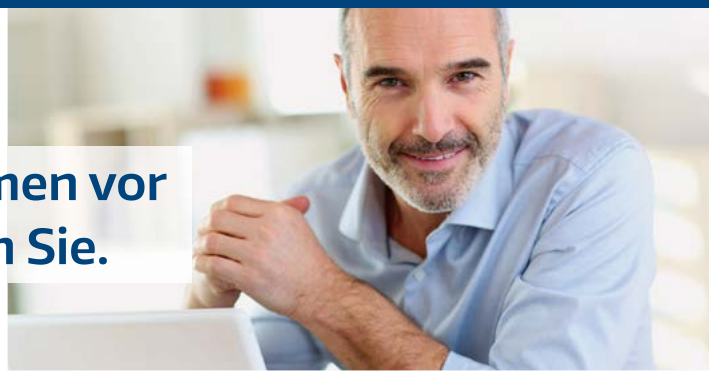
Die genannten Bereiche verdeutlichen nur einen Teil der Aspekte, die im Zusammenspiel von KI und Datenschutz zu berücksichtigen sind. Aber klar ist: Die Diskrepanz „zwischen der Unvollkommenheit des Menschen und der immer größer werdenden Perfektion seiner Maschinen“, von dem Philosophen Günter Anders als „Prometheisches Gefälle“ bezeichnet,[17] lässt den Anspruch gesellschaftlich, individuell und rechtlich (be)urteilen zu können, ob diese Maschinen gewollt sind, als Herkulesaufgabe erscheinen. Nur im Austausch mit allen Akteuren – insbesondere mit den Herstellern von KI-Anwendungen, den Institutionen, welche KI einsetzen, den Menschen, die von den Ergebnissen betroffen sind, mit Ethiker_innen und Philosoph_innen, die KI gesellschaftlich betrachten, mit den Gerichten, die über den zulässigen Einsatz von Anwendungen nach den rechtlichen Vorgaben, künftig auch nach den neuen europäischen Regelungen, zu entscheiden haben – wird es gelingen die Zukunft der KI gut zu gestalten. Um im Bild zu bleiben: Das prometheische Gefälle muss verkleinert werden, der Mensch muss stets die Kontrolle behalten. Dies erfordert zunächst Transparenz über die involvierte Logik einer KI und Transparenz über die Anwendung. Nur auf Basis von Transparenz kann die nötige Diskussion über den Einsatz von KI stattfinden.

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

CHRISTINA DENZ

ROTKÄPPCHEN UND DAS DATENSCHUTZPROBLEM

Kinderbuchautorin Tina Blase erklärt für den Bundesdatenschutzbeauftragten Informationsfreiheit und Datenschutz in vier Pixi-Büchlein

Schon Grundschulkinder haben Smartphones und sollten wissen, wie sie sich datensicher damit im Internet bewegen. Kinderbuchautorin Tina Blase hilft Kindern (und Eltern), abstrakte Begriffe wie „Informationsfreiheit", „privat" und „Datenschutz" zu verstehen.

Hätte Rotkäppchen dem Wolf nicht gesagt, wo die kranke Großmutter wohnt, wäre das Märchen der Gebrüder Grimm anders ausgegangen. Das dachte sich auch Greta, die mit ihren Freunden das Märchen im Theater aufführt. „Ich sag dir nicht, wohin ich gehe. Das ist nämlich privat", sagt Greta alias Rotkäppchen. Prompt trollt sich der Wolf.

„Dieses Märchen hat ein Datenschutzproblem", sagt Kinderbuchautorin Tina Blase und lacht. Sie hat für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vier Pixi-Bücher für Kinder verfasst und sich die Datenfüchse Greta, Yonas und Samuel ausgedacht. Die drei lernen, was privat ist und was man auf keinen Fall jemandem einfach so sagen sollte. Die Zeichnungen stammen von Horst Hellmeier.

Tina Blase hat neben „Das ist privat!" das Pixi-Buch „Aber warum?" zum Thema Transparenz für Kindergartenkind und die beiden Pixi-Wissen-Hefte „Was ist Datenschutz" und „Was ist Informationsfreiheit" für Grundschüler verfasst. In allen vier Bändchen lernen die Datenfüchse etwas über das Thema, etwa, warum sie nicht einfach so Bundestorwart Manuel Neuer anrufen können, um Tipps fürs Fußballspielen zu bekommen. Oder wie das Internet funktioniert, in dem sich heute „Computer durch die Luft" zufunken. Oder was Suchmaschinen sind.

Im Heft zur Informationsfreiheit erzählt Tina Blase die Geschichte vom Freibad Seepferdchen, das die Bürgermeisterin schließen will. Damit finden sich Greta, Yonas und Samuel aber nicht ab. Sie wollen mehr über die Hintergründe der Pläne erfahren, haken nach und bilden schließlich eine Bürgerinitiative zur Rettung des „Seepferdchens". Und nebenbei erfährt die kleine Leserschaft, was Datenschutzbeauftragte eigentlich so machen. Begleitend zu einzelnen Unterthemen hat die Autorin lustige Quiz entwickelt, die die kleinen Leserinnen und Leser zum Mitmachen anregen.

Für Tina Blase waren die Themen Datenschutz und Informationsfreiheit zumindest als Schreibauftrag des Carlsen-Verlags, der die Pixi-Büchlein herausgibt, neu. „Für das Projekt musste ich umfangreicher recherchieren als für andere Hefte", sagt sie. Sie fing bei der Bundeszentrale für politische Bildung an, las viel über aktuelle Datenschutzthemen, schrieb mehrere Entwürfe und ging dann mit der Kernidee von Greta, Yonas und Samuel in die Gespräche mit dem Projektteam beim BfDI.

Dort diskutierte das Team über Formulierungen und versuchte, griffige Erklärungen und konkrete Beispiele zu entwickeln. „Da ging es sehr um Details. Meine Aufgabe ist es, darauf zu achten, dass das Fachwissen für Kinder verständlich bleibt", sagt die Autorin und Lektorin aus Hamburg. Komplexe Begriffe sind deshalb in den beiden Pixi-Wissen-Heften erklärt, darunter „Was bedeutet transparent?", „Was sind Ämter und Behörden?" und auch „Akte", „Beschluss" und „Medien".

„Mitunter sind Begriffe, die Erwachsene selbstverständlich verwenden, für Kinder sehr abstrakt“, sagt Blase. „Das muss man bei Kinderbüchern zu solch komplexen Themen immer berücksichtigen.“

Mit der Reihe muss aber nicht Schluss sein. „Das Thema KI würde ich gerne für Kinder aufbereiten“, sagt Tina Blase, die für den Carlsen-Verlag auch schon Bücher zum Thema Mineralwasser, Turnabzeichen und Fahrradfahren verfasst hat. „KI und Datenschutz kindgerecht erzählen, das wäre sicher eine Herausforderung.“

Die Pixi-Bücher können kostenlos auf der Website des BfDI unter

▶ bfdi.bund.de/DE/Service/Publikationen/Pixi/Pixi_node.html

bestellt werden.

Über die Autorin

Christina Denz
ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News“.

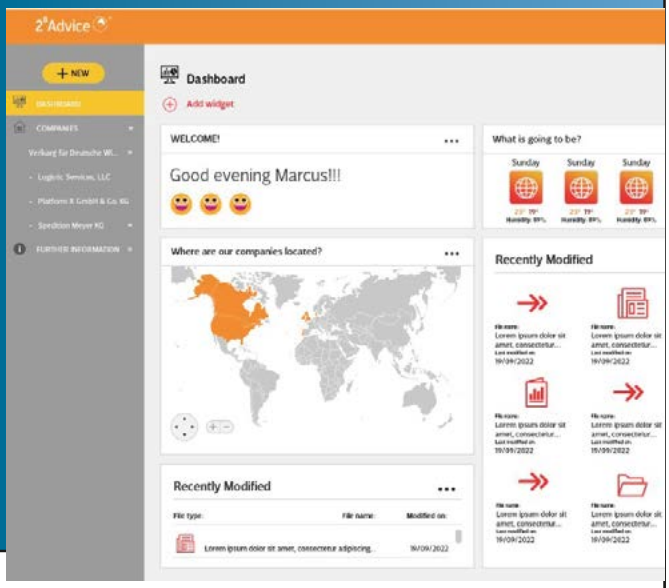
Anzeige

Eine neue Art von Datenschutzmanagementsoftware.

2B Advice
Integrated Risk Management Solutions

Die nächste Generation der bewährten Software 2B Advice PrIME kommt!

- Innovative KI-Lösung für noch weniger Aufwand
- Neue Nutzeroberfläche für eine noch einfachere Bedienung
- Von Datenschutzbeauftragten für Datenschutzbeauftragte entwickelt



Jetzt Kontakt aufnehmen & einer der Ersten sein, die PrIME Next Gen nutzen können:

TÜV SÜD ISO/IEC 27001 · CIPP iapp · ISO 19011 Auditor · iapp GOLD MEMBER

KARSTEN FÜLLHAASE

AUSTAUSCH, VERNETZUNG, SICHTBARKEIT

Viel Neues beim Europäischen Dachverbands EFDPO

Die erste EFDPO-Konferenz in Berlin wurde zum Treffpunkt für Mitglieder aus ganz Europa.
1. Reihe (v.l.n.r.): Judith Leschanz (Österreich), Spiros Tassis (Griechenland), Dr. Kai-Uwe Loser (Deutschland), Dr. Philipp Mittelberger (Liechtenstein);
2. Reihe (v.l.n.r.): Thomas Spaeing (Deutschland), Pavol Szabó (Slowakei), Klaus Mönikes (Deutschland), Pierre-Yves Lastic (Frankreich), Karsten Füllhaase (Deutschland)

Bereits 2018 hatte der BvD begonnen, Gespräche mit Verbänden in anderen EU-Staaten zu führen, die wie der BvD als Berufsverbände die Interessen der im Datenschutz tätigen Personen vertreten und fördern. Ziel war die Gründung eines unabhängigen Dachverbandes auf EU-Ebene. Nach Arbeitstreffen in Lissabon, Prag und Wien wurde die European Federation of Data Protection Officers (EFDPO) im Anschluss an die BvD-Verbandstage am 7. Juni 2019 in Berlin gegründet.

Die ersten Jahre des in Brüssel ansässigen Verbands waren geprägt durch organisatorische Meilensteine wie die Eintragung als belgische Non-Profit-Institution „Association internationale sans but lucratif " (AISBL) per königlichem Erlass. Zu den formalen Schritten der Gründung gehörte auch, dass das Logo als Unionsmarke beim Amt der Europäischen Union für geistiges Eigentum (EUIPO) registriert wurde. Ein besonderer Fokus der Anfangsjahre lag zudem auf der Gewinnung neuer Mitgliedsverbände. Zusätzlich zu den acht Gründungsmitgliedern – neben dem BvD sind dies Verbände aus Österreich, Frankreich, Portugal, Tschechien, der Slowakei, Griechenland und Liechtenstein – haben sich mittlerweile neun weitere Verbände angeschlossen. Sie stammen aus Deutschland, Kroatien, der Schweiz, Dänemark, Schweden, Finnland und sogar aus Brasilien und Französisch-Polynesien. Teilweise sind dies ordentliche Mitglieder, teils assoziierte Mitglieder mit allen Rechten außer dem Stimmrecht bei der Mitgliederversammlung.

Gerade in der Anfangszeit musste die EFDPO viel Zeit und Engagement in diese organisatorischen Erforderlichkeiten und Aufbauarbeiten investieren. Aber seit einiger Zeit stellt der Verband auch viele Dinge auf die Beine, die Wirkung und Sichtbarkeit entwickeln. Das gilt für die politische Arbeit und die allgemeine Öffentlichkeitsarbeit einerseits, andererseits auch für die Aktivitäten in Richtung Mitgliedervernetzung und Wissenstransfer.

Politische Arbeit und PR-Maßnahmen für den Datenschutzbeauftragten

Auf politischer Ebene hat sich die EFDPO gleich zu Beginn an der Evaluation des DSGVO 2020 beteiligt sowie Stellungnahmen bei mehreren Konsultationen des Europäischen Datenschutzausschusses (EDSA) eingereicht. Zuletzt hat die EFDPO beispielsweise Positionen zum Data Act und der Initiative der EU-Kommission zur Präzisierung der Verfahrensregeln für die Durchsetzung der DSGVO erarbeitet. Dass diese Arbeit wahrgenommen wird, zeigt sich nicht zuletzt daran, dass die EFDPO für ein Experteninterview im Zuge der Erstellung des Jahresberichts des EDSA herangezogen wurde, um Feedback für dessen Arbeit einzubringen. Für die kommenden Monate steht nun die Vorbereitung und Abstimmung eines Positionspapiers zur DSGVO-Evaluation 2024 auf dem Plan.

Auch PR-Maßnahmen, die das Image des Datenschutzbeauftragten fördern, gehören zum Betätigungsfeld der EFDPO. Dazu zählen beispielsweise kleine Kampagnen rund um den Europäischen Datenschutztag am 28. Januar sowie die Etablierung des von der EFDPO ausgerufenen „International DPO Day“ am 25. Mai, den der Verband mit Presseinformationen und Social-Media-Aktivitäten öffentlichkeitswirksam zelebriert. Mit dem DPO Day schafft der Verband ein Bewusstsein dafür, dass mit der DSGVO die Funktion des betrieblichen und behördlichen Datenschutzbeauftragten erstmals flächendeckend in allen EU-Mitgliedsstaaten eingeführt wurde. Er bietet gleichzeitig einen Anlass für die EFDPO, um Forderungen für den Berufsstand zu formulieren, beispielsweise eine Aufnahme des Berufs in das „International Classification Type of Professions“ der International Labor Organization.

Beim Privacy Symposium in Venedig hatte eine Delegation der EFDPO Gelegenheit, sich mit der (damaligen) Vorsitzenden des EDSA, Andrea Jelinek, auszutauschen.

Podiumsdiskussion der EFDPO zum Thema “Die Zukunft der Datenschutzbeauftragten” beim Privacy Symposium in Venedig

Kostenlose Online-Events

Ein weiteres Hauptziel des Verbandes ist es, die Datenschutzbeauftragten der EU-Mitgliedsstaaten miteinander zu vernetzen. Gerade hier hat sich beim Dachverband in den letzten Monaten viel getan. Zusätzlich den monatlichen (digitalen) Arbeitstreffen der EFDPO hat der Verband allein in diesem Jahr bereits zu fünf Online-Events zu verschiedenen aktuellen Themen eingeladen. Neben internationalen Datentransfers, stand unter anderem der Europäische Gesundheitsdatenraum und zuletzt das Thema Metaverse im Zentrum der Vorträge und Diskussionspanels. Dabei waren neben Experten aus den EFDPO-Mitgliedsverbänden (zum Beispiel BvD-Vorstand Christoph Bausewein) auch renommierte Gäste wie Max Schrems zu hören. Alle diese Online-Veranstaltungen sind für Mitglieder der EFDPO-Verbände also auch für BvD-Mitglieder kostenlos. Die Termine finden sich auf den Webseiten der EFDPO und des BvD sowie in den BvD-Mitgliederinformationen und den Social Media Kanälen beider Verbände.

Nach einer anfänglichen – auch pandemiebedingten – Konzentration auf Online-Formate, kommen aktuell vermehrt Präsenzveranstaltungen im Terminkalender der EFDPO hinzu. Dabei zeigt sich, wie hilfreich und wichtig bei aller Digitalisierung der persönliche Kontakt für die Vernetzung ist und bleibt. Das gilt sowohl für die Vernetzung innerhalb des Verbandes als auch für den Kontakt mit externen Stakeholdern.

Partnerschaften mit internationalen Kongressen in Venedig und Brüssel

Um bei beschränkten finanziellen Mitteln (jeder Mitgliedsverband zahlt pro Jahr die eigene Mitgliederzahl multipliziert mit vier Euro) größtmögliche Wirkung zu generieren, setzt die EFDPO auf Kooperationen mit strategischen Partnern. Im Veranstaltungsbereich sind die die beiden internationalen Kongresse Privacy Symposium in Venedig und CPDP in Brüssel.

Beim Privacy Symposium war die EFDPO im vergangenen April bereits zum zweiten Mal einer der „Key Partner“. Weitere wichtige Partner - neben der EFDPO - waren der Europarat, das Europäische Zentrum für Zertifizierung und Datenschutz,

CLUSIT, die European Law Students' Association, das Italienische Institut für Datenschutz und Datenverwertung, das IoT Forum zum Austausch über das Internet of Things und die EU-Initiative „Next Generation Internet of Things" (NGIoT).

Neben den EFDPO-Vorstandsmitgliedern Judith Leschanz und Philipp Mittelberger und dem EFDPO-Generalsekretär Pierre-Yves Lastic nahmen auch mehrere Mitglieder von EFDPO-Mitgliedsverbänden an der Konferenz teil. Die Themen waren breit gestreut und reichten von Sandbox und Zertifizierung über Überwachung und Telemarketing bis hin zur globalen Konvergenz der Datenschutzvorschriften. Eine Erkenntnis, nicht nur aus den Panels, sondern auch aus den vielen interessanten Gesprächen am Rande der Konferenz: Alle Kollegen in den EU-Ländern stehen vor den gleichen Herausforderungen, sind allerdings mit nationalen Gesetzen und Meinungen der Datenschutzbehörden konfrontiert, die nicht ganz identisch sind.

Judith Leschaz, Vorsitzende des österreischichen Vereins Privacyofficers.at und Dr. Philipp Mittelberger, Präsident des Datenschutzvereins Liechtenstein.

In einer vom EFDPO veranstalteten Podiumsdiskussion wurde das Thema „Die Zukunft der Datenschutzbeauftragten" erörtert. Es gab auch einige praktische Ratschläge zum Datenschutzaustausch mit China und Indien, und natürlich wurde das bevorstehende Trans-Atlantic Data Privacy Framework (und die künftige Rolle Großbritanniens) intensiv diskutiert. Auf internationaler Ebene wurde die Entwicklung des Datenschutzes in Asien und Lateinamerika erörtert, und es gab Stellungnahmen von europäischen und internationalen Datenschutzbehörden, die in beachtlicher Vielzahl vor Ort vertreten waren.

Auch das Networking kam nicht zu kurz, und es wurden viele neue Kontakte geknüpft. Zum ersten Mal organisierte EFDPO ein Get-together für die Teilnehmer des Privacy Symposium, das sehr gut besucht war. In diesem Zusammenhang hatte die EFDPO auch die Gelegenheit, sich mit der (damaligen) Vorsitzenden des Europäischen Datenschutzausschusses, Andrea Jelinek, auszutauschen.

Auch nächstes Jahr plant die EFDPO eine Kooperation mit dem Privacy Symposium, dass voraussichtlich vom 10. bis 14. April 2024 stattfinden wird. BvD-Mitglieder profitieren von

EFDPO-Generalsekretär Pierre-Yves Lastic

einer ermäßigten Teilnahmegebühr. Der entsprechende Promotion-Code wird rechtzeitig kommuniziert werden.

CPDP steht für „Computers, Privacy and Data Protection" (Computer, Privatsphäre und Datenschutz) und ist eine jährliche dreitägige Konferenz in Brüssel, die den neuesten Stand der rechtlichen, regulatorischen, akademischen und technologischen Aspekte des Schutzes der Privatsphäre und des Datenschutzes vermittelt. Sie fördert ein dynamisches Zusammentreffen verschiedener Interessengruppen aus der ganzen Welt, unter anderem verstärkt aus dem universitären Bereich, um Ideen und Diskussionen über neu aufkommende Probleme und die neuesten Entwicklungen zu führen.

Die 16. Ausgabe des CPDP fand vom 24. bis 26. Mai 2023 statt, und zum ersten Mal war die EFDPO ein Event Partner und hat auch hier ein eigenes Panel zum umfassenden Programm beigesteuert, das auf extrem große Resonanz stieß. Diskutiert wurde, wie sich die neue EU-Digitalgesetzgebung auf die Rolle der Datenschutzbeauftragten und der Aufsichtsbehörden auswirken wird. František Nonnemann vom tschechischen Datenschutzverband, EFDPO-Generalsekretär Pierre-Yves Lastic, Michael Will, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, und Judith Leschanz von Privacyofficers.at bildeten das hochkarätige Panel, dessen Erkenntnisse sich viel-

František Nonnemann vom tschechischen Datenschutzverband, EFDPO-Generalsekretär Pierre-Yves Lastic, Michael Will, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, und Judith Leschanz von Privacyofficers.at bildeten das hochkarätige EFDPO-Panel bei der CPDP in Brüssel

BvD-Vorständin Regina Mühlich und EFDPO Vizepräsidentin Judith Leschanz bei der Abendveranstaltung der EFDPO-Konferenz in Berlin

leicht so zusammenfassen lassen:

- Nutzen Sie bei den neuen Rechtsakten die Erfahrungen aus der DSGVO-Implementierung.
- Vermeiden Sie einen Silo-Ansatz, die DSGVO ist „nur" Teil eines breiteren regulatorischen Rahmens.
- Vorsicht vor nationalen Alleingängen bei der zu etablierenden Aufsichtsstruktur.

Erste eigene EFDPO-Konferenz in Berlin

Ein Highlight im diesjährigen Veranstaltungskalender der EFDPO war neben den Kongress-Kooperationen in Brüssel und Venedig die erste eigene Konferenz der EFDPO. Sie fand am 9. und 10. Mai im Rahmen der BvD-Verbandstage statt. Sechs Vorträge und Diskussionspanels mit Expertinnen und Experten aus Deutschland, Frankreich, der Slowakei und der Tschechischen Republik standen auf dem Programm. Dabei ging es unter anderem um die koordinierte Durchsetzungsaktion des EDSA zur Stellung des Datenschutzbeauftragten aber vor allem um die zahlreichen neuen Rechtsakte, die im Zusammenhang mit der europäischen Digitalstrategie gerade verabschiedet wurden oder kurz vor der Verabschiedung stehen. Insbesondere der Data Act wurde dabei von mehreren Referenten aus unterschiedlichen Blickwinkeln beleuchtet. Ein Stimmungsbild, das zum Abschluss des Kongresses von den Teilnehmenden eingeholt wurde, zeigte eine durchweg positive Resonanz der internationalen Gäste. Auch von vielen BvD-Mitgliedern wurde das neue englischsprachige Angebot, das in der Teilnahmegebühr der Verbandstage inkludiert war, sehr gut angenommen.

Großer Zulauf beim EFDPO-Panel auf der CPDP in Brüssel

Im Anschluss an den Kongress hielt die EFDPO zudem noch ihre ordentliche Mitgliederversammlung ab. Auf der Tagesordnung standen unter anderem die Wahlen des Vorstands. Für den BvD wurde Thomas Spaeing als Präsident der EFDPO einstimmig im Amt bestätigt und wird nun gemeinsam mit acht weiteren Vorständen für drei weitere Jahre die Entwicklung des Dachverbands vorantreiben.

AUSBLICK

Nach dem großen Erfolg des Berliner EFDPO-Kongresses werden bereits die nächsten Präsenzveranstaltung geplant. Neben einem EFDPO-Panel bei einem Kongress am 5. Oktober in Prag ist ein Fachkongress zum Thema Gesundheitsdaten am 24. und 25. Oktober 2023 in Paris in Vorbereitung. Geplant ist, Aufzeichnungen der Vorträge und Diskussionsrunden im Nachgang allen Mitgliedern der EFDPO-Mitgliedsverbände online zur Verfügung zu stellen, so dass auch diejenigen davon profitieren, die nicht nach Paris reisen können. Die Konzeption des Kongresses ist das erste Projekt der EFDPO-Arbeitsgruppe „Health Data". Weitere Arbeitsgruppen und Ausschüsse der EFDPO beschäftigen sich mit den Themen Cybersecurity, Künstliche Intelligenz sowie Zertifizierung/Berufsbild. Ihre Arbeit nimmt nun ebenfalls mehr und mehr Fahrt auf.

▶ efdpo.eu

▶ E-Mai: office@efdpo.eu

Über den Autor

Karsten Füllhaase
ist Geschäftsführer des BvD. Neben der Leitung und Betreuung der Geschäftsstelle begleitet er vor allem die Entwicklung des europäischen Dachverbands EFDPO und unterstützt den Vorstand bei der Ausschussarbeit sowie der politischen Verbandskommunikation in Berlin. Der Kulturwissenschaftler ist Kommunikationsprofi mit 15-jähriger Erfahrung in leitenden Positionen für Stiftungen und gemeinnützige Gesellschaften.

BvD-Mitglieder, die sich aktiv in die englischsprachigen Arbeitsgruppen einbringen möchten, sind herzlich eingeladen, sich bei BvD-Geschäftsführer Karsten Füllhaase zu melden.

▶ karsten.fuellhaase@bvdnet.de

CHRISTINA DENZ

SPANNEND UND AUFKLÄREND: JURY VERGIBT DIE DAME 2022

Eine Gemeinschaftsrecherche über Googles Datenmissbrauch gewinnt die 6. Runde des Datenschutz Medienpreises

DAME-Preisverleihung auf den BvD-Verbandstagen im Mai 2023 in Berlin

Vier Monate recherchierte ein interdisziplinäres Team der „Süddeutschen Zeitung" zum Datenmissbrauch von Google. Daraus entstand der Themenschwerpunkt „Was Google über uns weiß" aus Berichten, Hintergründen und Grafiken. Das Gesamtpaket der intensiven Arbeit hat bei der 6. Preisverleihung des Datenschutz Medienpreises (DAME) 2022 die Jury überzeugt. Das Recherche-Team gewann den mit 3.000 Euro dotierten Hauptpreis.

Bei der Preisverleihung am 9. Mai im Rahmen der BvD-Verbandstage in Berlin nahmen Berit Kruse, Sophie Menner und Marie-Louise Timcke den Preis für das insgesamt acht-köpfige Team entgegen, eingereicht hatte das Themenpaket für das Ressort Wirtschaft David Wünschel. In den Texten gehen die Journalisten der Frage nach, wie Google seinen wohl größten Datenschatz der Welt verwendet und welche Macht der Konzern damit erreicht.

Das sagt Jury-Mitglied Tobias Meisel über den Hauptpreis:

Der Beitrag legt die Marktmacht von Google schonungslos offen. Er sensibilisiert die Lesenden in einem sehr kurzweiligen Format für den Umgang mit den eigenen Daten im Internet. Der Beitrag ist sehr tiefgründig recherchiert, die Betrachtung mehrerer Seiten machen ihn sehr wertvoll und zu einem verdienten Gewinner.

Dr. Christoph Bausewein, Geschäftsführer der privacy4people gGmbH, die Vertreterinnen des Gewinner-Teams und Moderator Ralph Caspers.

Marie-Luise Timcke (Hauptpreis)

„Die Arbeit in interdiziplinären Teams macht das Ergbnis einfach besser, weil viel Knowhow aus unterschiedlichen Ressorts und Erfahrungen zusammenkommt. Klar ist es eine Herausforderung zusammen ein Text zu schreiben. Aber da auch im Journalismus Leute mit Fachkenntnissen immer weniger werden, ist die Team-Arbeit für die Themen eine gute Lösung."

Das sagt Jury-Mitglied Lars Kolan über den Hauptpreis:

Neben der Tatsache, dass der Text einen von Anfang an fesselt, haben mich vor allem die umfangreichen Analysen und Recherchearbeiten beeindruckt. Die Erläuterungen zum Real-Time-Bidding waren sehr interessant, vor allem zur möglichen politischen Einflussnahme von Google durch das gezielte Ranking von politischer Werbung an der obersten Stelle der Suchergebnisse, ohne dass die mit dem eigentlichen Suchbegriff zu tun haben. Das hat mich richtig wachgerüttelt und war für mich etwas Neues, das mir mit Blick auf die Zukunft große Sorge bereitet.

Als Bester Beitrag Jugend wertete die Jury den Kurzfilm „Gemeinsam für die Privatsphäre. Damit du mehr Zeit zum Fußball spielen hast" von Andrina Schmid und Samuel Wetter. In dem Clip folgen wir „Max" beim Online-Shopping, wir sehen ihn, wie er Beiträge postet und seinem Lieblingsfußballverein online folgt. Die Kernaussage: Wir verhalten uns alle wie Max. Doch die Apps, die wir benutzen, beobachten „auch deine Likes, Kommentare und was du etwas länger anschaust, kurz: dein Verhalten", heißt es im Abspann des Films. Je mehr Minuten wir im Netz verbringen, „desto besser werden die Medien darin dich zu verführen noch mehr online zu sein." Am Ende fehlt uns Zeit, befinden Andrina und Samuel in ihrer Arbeit, die bereits vom Kanton Zürich einen Preis erhielt.

Andrina Schmid und Samuel Wetter mit privacy4people-Geschäftsführer Dr. Christoph Bausewein

Das sagt Jugend-Juror Eric Hohenadel zum Besten Beitrag Jugend:

Der kreative und anschauliche Kurz-Film macht deutlich, wie gerade Jugendliche durch die tagtägliche Nutzung sozialer Medien beeinflusst werden und ihre tiefste Privatsphäre verletzt werden kann. Der junge Protagonist spiegelt den Alltag vieler Jugendlicher und zeigt, dass wir selbst und unsere Daten zum Produkt werden können, wenn wir zum Beispiel eine App herunterladen.

Andrina Schmid (Bester Beitrag Jugend)

„Wir wollten schon lange ein Projekt realisieren über ein Thema, das online eine Rolle spielt. Als wir dann die Ausschreibung des Kanton Zürichs gelesen haben, kamen wir schnell auf unsere Geschichte. Am Ende haben wir einen halben Tag gedreht und zwei Tage an Schnitt und Text gearbeitet."

Als beste Audio-Reportage lobte die Jury die Arbeit „Identitätsdiebstahl über Jobportale" der Fernseh- und Radio-Journalistin Sabina Wolf vom Bayerischen Rundfunk (BR). Sie recherchierte zunächst für die ARD-Fernsehsendung „report München" und verfasste im Anschluss aus dem Material einen Radiobeitrag für die BR-Reihe „Funkstreifzug".

Sabina Wolf mit privacy4people-Geschäftsführer Dr. Christoph Bausewein und Moderator Ralph Caspers.

Dabei sprach sie mit Betroffenen, die sich auf einem bekannten Jobportal auf eine Anzeige bewarben, dabei persönliche Daten preisgaben und durch eine Ausweisfotografie einen Identitätsdiebstahl mit verheerenden Folgen erlitten. Das perfide: Die Anzeigen missbrauchten Namen und Corporate Design von echten Firmen, so dass die Opfer keinen Verdacht schöpften. Oft merkten die Betroffenen den Eingriff erst, als die Polizei gegen sie ermittele.

> Sabina Wolf (Bester Beitrag Audio)
>
> *„Ich selbst bin mittlerweile sehr vorsichtig wenn es um meine Daten im Internet geht, weil ich seit 15 Jahren über Datenklau und Datenmissbrauch berichte. Das sollten auch Bewerber sein, die im Internet auf Jobangebote antworten. Spätestens wenn jemand den Ausweis als Fotokopie oder als Foto verlangt, sollte man hellhörig werden. Da gibt es andere Wege sich zu legitimieren. Helfen könnte eine Zwei-Faktor-Authentifizierung wie beim Homebanking oder schlicht ein Festnetzanruf bei der Firma selbst."*

Sabina Wolf freute sich über den Preis, „weil mir das Thema sehr am Herzen liegt", wie sie nach der Bekanntgabe sagte. Die Opfer müssten selbst nachweisen, dass sie nicht in Geldwäsche oder andere kriminelle Taten verwickelt seien, die unter ihrem Namen verübt werden. Dies sei für sie eine traumatische Erfahrung. Gerade junge Menschen schöpften oft keinen Verdacht, da für sie Online-Bewerbungen zum Alltag gehörten. Dabei kritisierte Sabina Wolf auch die aktuelle Rechtslage, dass Jobportale Anzeigen nicht prüfen müssten. „Die Politik muss viel mehr machen, um die Menschen vor Identitätsdiebstahl zu schützen", forderte sie.

Das sagt Jury-Mitglied Barbara Thiele über den Besten Beitrag Audio:

Sabina Wolf zeigt ein umfassendes und zugleich alarmierendes Bild einer perfiden Betrugsmasche, bei der die Opfer, im guten Glauben mit einem seriösen Unternehmen zu kommunizieren, erst persönliche Daten und ihre Identität preisgeben und dann selbst kriminalisiert werden. Denn in ihrem Namen begehen die Täter umfangreiche Straftaten, mit katastrophalen persönliche Folgen. Der Beitrag zeigt auch, wie wichtig es ist, sensibel und sparsam mit den eigenen Daten umzugehen, egal wie vertrauenswürdig der potenzielle Arbeitgeber erscheint.

Insgesamt hatten sich 42 Einreichungen um die DAME 2022 beworben. „Es war eine Herausforderung sich bei den vielen guten Beiträgen für drei zu entscheiden" sagte Jury-Mitglied Barbara Thiel. Die Lektüre und Sichtung der Beiträge nahm laut Lars Kolan vom Deutschen Spendenrat rund 50 Stunden in Anspruch. Themenvielalt und Wissensvermittlung bezeichnete er als immens, „man konnte wirklich aus jedem Beitrag etwas mitnehmen".

Darunter waren erneut viele spannende und kreative Einreichungen, wie BvD-Vorstandsvorsitzender Thomas Spaeing sagte. Die Beiträge waren allesamt unterhaltsam, waren geistreich, gut verständlich und führten oft zu einer nachhaltigen Erkenntnis, laut BvD-Vorstandsvorsitzendem Thomas Spaeing. Das Thema Datenschutz sei mittlerweile in allen Altersgruppen angekommen. „Genau das wollen wir erreichen: Datenschutz als Selbstverändlichkeit."

Der BvD rief die DAME 2017 ins Leben. Seit 2020 wird er von der gemeinnützigen privacy4people GmbH fortgeführt und seit November 2018 von der DATEV-Stftung Zukunft gefördert. Der Deutsche Spendenrat stiftet einen Sonderpreis. Kooperationspartner ist die EU-Initiative klicksafe.

NÄCHSTE RUNDE FÜR DIE DAME

Der Datenschutz Medienpreis geht in die siebte Ausschreibung. Ab sofort können sich Medienschaffende, Kreative und auch Gruppen um die DAME 2023 bewerben. Die Einreichungen sollten einen Aspekt aus dem Datenschutz verständlich und anschaulich für eine Zielgruppe vermitteln.

Einsendeschluss ist der 31. Dezember 2023.

Über die Autorin

Christina Denz

ist Journalistin, Kommunikationsberaterin und Redakteurin der „BvD-News".

Hier können Sie alle 42 Einreichungen zur DAME 2022 einsehen.

▶ bvdnet.de/wp-content/uploads/2023/03/Uebersicht_Einreichungen-DAME-2022.pdf

Medienpartner:

Förderer:

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

Datenschutzkonferenz 2023

Praxis | Recht | Innovation

» 27.-29. September 2023 | Hotel Kö59 Düsseldorf

Auch dieses Jahr wieder mit dabei: das Datenschutz-Quiz mit Dr. Stefan Brink und Alvar Freude

Es erwarten Sie u.a. diese Themen:

- Wer haftet für Datenschutzverstöße?
- Data Act vs. DSGVO: Schnittstellen und Konflikte
- Update internationale Datentransfers
- Aktuelle Entwicklungen in DSGVO-Bußgeldverfahren
- Neuigkeiten zum Beschäftigtendatenschutz
- Betroffenenrechte im Webseitenkontext
- Meldung von Datenschutzverstößen
- Aktuelle EuGH-Entscheidungen und -Verfahren zum Datenschutz

Freuen Sie sich auf neue Impulse durch:

Dr. Jens Ambrock

Dr. Isabelle Brams

Dr. Stefan Brink

Stephan Hansen-Oest

Peter Hense

Dr. Nina Elisabeth Herbort

Meike Kamp

Dr. Flemming Moos

Dr. Aileen Pasquariello

Frederick Richter

Dr. Dominik Sorber

Jan Spittka

Dr. Paul Voigt

Tim Wybitul

Und vielen weiteren Referentinnen und Referenten.

Melden Sie sich jetzt an! www.datenschutzkonferenz.de

Anmeldungen & organisatorische Rückfragen an:
Herrn Jasha Baniashraf
Deutscher Fachverlag GmbH
Telefon: 069/7595-2773
Fax: 069/7595-1150
E-Mail: Jasha.Baniashraf@dfv.de

Medienpartner:

DATENSCHUTZ-BERATER

Kommunikation & Recht

Compliance Berater

VORSTAND IM AMT BESTÄTIGT

Mitgliederversammlung wählt BvD-Vorstand für weitere zwei Jahre

Am 8. Mai 2023 fand die diesjährige ordentliche Mitgliederversammlung des BvD in Berlin statt. Auf der Tagesordnung stand die Wahl des Vorstands, dessen Mitglieder geschlossen erneut zur Wahl angetreten waren und mit überwältigender Zustimmung für zwei weitere Jahre im Amt bestätigt wurden. Weiteres Thema war der Beschluss einer neuen Wahlordnung. Sie wird zukünftig die Modalitäten von Wahlen im Rahmen der Mitgliederversammlung regeln. In Kraft treten wird sie zeitgleich mit der neuen Satzung des BvD und als wichtigste Änderung mit sich bringen, dass Vorstandswahlen zukünftig immer geheim abgehalten werden und der Vorstand für jeweils drei statt bisher zwei Jahre gewählt wird.

Und die neue Satzung? Die wurde bereits im Oktober 2022 in der außerordentlichen Mitgliederversammlung in Stuttgart beschlossen und anschließend beim zuständigen Amtsgericht Charlottenburg eingereicht. Per Schreiben vom 4. April 2023 informierte das Amtsgericht den BvD jedoch, dass aufgrund einiger Beanstandungen die Eintragung nicht erfolgen kann. Es gilt bis auf Weiteres die Satzung in der Fassung vom 21. Oktober 2015. Zur Beschlussfassung über die vom Amtsgericht geforderten Änderungen an der Neufassung der Satzung gab es am 6. Juni 2023 eine außerordentliche Mitgliederversammlung in Berlin. Nach § 13 Abs. 1 S. 1 der Satzung kann über eine Satzungsänderung nur entschieden werden, wenn zehn Prozent und mindestens zehn stimmberechtigte Mitglieder anwesend sind.

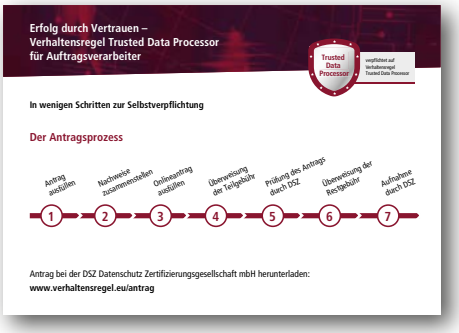
Die erforderlichen zehn Prozent wurden nicht erreicht, so dass eine weitere außerordentliche Mitgliederversammlung erforderlich ist, die am 17. Oktober 2023 stattfinden und in jedem Fall beschlussfähig sein wird, so dass einer anschließenden Eintragung durch das Amtsgericht nichts im Wege steht. Die beantragten Änderungen finden BvD-Mitglieder in ihrer Einladung zur Mitgliederversammlung und im Mitgliederbereich der BvD-Website. *kfh*

„TRUSTED DATA PROCESSOR“ IM ÜBERBLICK

Für die nationale Verhaltensregel „Trusted Data Processor“ hat der BvD eine neue Handreichung entwickelt. Auf vier Seiten erklären grafische Darstellungen im Überblick, wie Auftragsverarbeitende das Qualitätssiegel erhalten können. Die Handreichung erläutert prägnant und gut verständlich unter anderem die Vorteile der Zertifizierung, deren Kosten und den eigentlichen Zertifizierungsprozess.

Insbesondere soll die Übersicht Datenschutzbeauftragte unterstützen Entscheidern im Unternehmen oder einem Kunden den Prozess verständlich zu erklären, so dass alle Beteiligte ein gemeinsames Verständnis für den Antragsprozess entwickeln können.

Der BvD hat die Verhaltensregel maßgeblich mit entwickelt. Eine Beschreibung des detaillierten Prozesses finden Sie außerdem in der BvD-News Ausgabe 1/23. *chd*



Die vier übersichtlichen Charts können Sie herunterladen unter:

▶ bvdnet.de/wp-content/uploads/2023/06/Handreichung-Trusted-Data-Processor.pdf

BVD-BERATUNGSHOTLINE FÜR MITGLIEDER GESTARTET

Der BvD bietet seinen Mitgliedern seit dem 16. Mai 2023 zu festen Zeiten jeweils von Dienstag bis Donnerstag eine Telefonberatung zu Fragen aus der Berufspraxis an. Für die kostenlose rund. 15-minütige juristische Ersteinschätzung haben wir die Kanzlei SDS Rechtsanwälte Sander Schöning PartG mbB beauftragt. Die Themen der ersten Beratungen reichten von Fragen zu medizinischen Daten, über Datenschutzerklärungen für Internetseiten und Löschungsverlangen im Kontext des Medienprivilegs bis zur Geltung der DSGVO in der Schweiz und Datenschutz-Folgenabschätzungen bei Zeiterfassungssystemen. Gerade für Berufseinsteiger ist die Hotline ein hilfreiches Angebot bei der Einschätzung von neuen oder schwierigen Sachverhalten.

Manchmal braucht man einfach nur einen Sparringspartner um ein Problem einmal aus einer anderen Sicht mit zu beleuchten. *jh*

BVD-BERATUNGSHOTLINE

Der BvD und die beratenden Anwälte der SDS Rechtsanwälte Sander Schöning Part GmbH sehen einen gelungenen Start und freuen sich auf weitere Anfragen. Details zu der dienstags, mittwochs und donnerstags erreichbaren Hotline sowie die Telefonnummer finden BvD-Mitglieder im internen Bereich der BvD-Webseite.

LINK-TIPPS

Gesetze und Verordnungen des Bundes

Seit dem 1. Januar 2023 werden Gesetze und Verordnungen des Bundes nur noch online verkündet:

▶ recht.bund.de/de/home/home_node.html

European Essential Guarantees Guide

A Global Look at Fundamental Rights to Privacy & Data ProtecOon

▶ essentialguarantees.com/

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

EIN ALGORITHMUS HAT KEIN TAKTGEFÜHL

WO KÜNSTLICHE INTELLIGENZ SICH IRRT, WARUM UNS DAS BETRIFFT UND WAS WIR DAGEGEN TUN KÖNNEN

Katharina Zweig

Die Referenten und Moderatoren erhalten vom BvD immer ein kleines Dankeschön. Bei den Verbandstagen im Mai 2023 in Berlin gab es diesmal als Lesestoff „Ein Algorithmus hat kein Taktgefühl" von Katharina Zweig.

Algorithmen bestimmen zunehmend den Alltag. Die Entwicklung hin zu einer technisierten Gesellschaft hat viele Facetten. Folgen drohen vor allem dort, wo Künstliche Intelligenz (KI) menschliches Verhalten bewerten und vorhersagen soll. Müssen wir Angst vor Algorithmen, Big Data oder KI haben? Nein, sagt die Autorin. Aber wir sollten verstehen, worum es geht. Nur so können wir mitreden und uns gezielt einmischen. Das Buch ist unterhaltsam geschrieben und erklärt anhand vieler Beispiele ein komplexes Thema. Es erklärt, was sich hinter den einzelnen Begriffen verbirgt und gibt mögliche Antworten.

Das Buch besteht aus drei Teilen:

Der erste Teil, „Der Werkzeugkoffer", stellt die naturwissenschaftliche Methode der Erkenntnisgewinnung und den sogenannten „Werkzeugkoffer" vor. Im zweiten Teil, „Das kleine ABC der Informatik", befindet sich der Leser im Maschinenraum. Er beschreibt den Zusammenhang zwischen Algorithmen, Big Data und Computerintelligenz. Im dritten Teil „Der Weg zu besseren Entscheidungen – mit und ohne Maschinen" geht es um die Fragen, wo und wie die Ethik in den Rechner kommt und wie man diesen Prozess bestmöglich gestaltet. Es wird beschrieben, warum Algorithmen problematisch sein können. Dabei werden verschiedene Lösungsansätze präsentiert, z.B. die Frage „Wie kommt die Diskriminierungen in den Rechner?". Um mit Diskriminierung umgehen zu können sowie „Sollen Maschinen Menschen bewerten dürfen?", ist es notwendig erst die Interpretation der maschinellen Resultate und die Auswahl der Aktionen in der langen Kette der Verantwortlichkeiten zu bestimmen. Es geht darum zu erkennen, welchen sozialen Nutzen ein System hat (algorithmische Entscheidungssysteme). Dieser letzte Teil ist für mich der interessanteste. Hier beleuchtet die Autorin die soziologischen und gesellschaftlichen Aspekte unter Berücksichtigung der technischen Gegebenheiten und Voraussetzungen.

Katharina Zweig
EIN ALGORITHMUS HAT KEIN TAKTGEFÜHL

Heyne

5. Auflage
319 Seiten, Paperback
20,00 Euro (brutto)
ISBN: 978-3-453-20730-1

Die Autorin, Katharina Zweig, leitet als Universitätsprofessorin am Fachbereich Informatik der TU Kaiserslautern das „Algorithm Accountability Labs". Sie hat den Studiengang „Sozioinformatik" ins Leben gerufen und ist Mitglied der Enquete-Kommission des Bundestages zum Thema „Künstliche Intelligenz".

Fazit:

Das Buch ist kein „Lehrbuch". Wer also tiefe technische Einblicke erwartet braucht das Buch nicht zu lesen. Wer aber die Komplexität von KI und Algorithmen auf verständliche und unterhaltsame Weise erklärt bekommen und verstehen möchte, um mitreden und mitdiskutieren zu können, für den ist dieses Buch ideal.

Zum Buch noch etwas für „Augen und Ohren": Vortrag zum Buch „Zwischen Utopie und Dystopie" auf YouTube:

▶ youtube.com/watch?v=Af3B6-oR1W4
(Start bei 11:12 min.)

DIE DIGITALE TRANSFORMATION DES QUALITÄTSMANAGEMENTS

POTENTIALE NUTZEN, STRATEGIEN ENTWICKELN, QUALITÄT OPTIMIEREN

Gernot Freisinger, Oliver Jöbstl, Bernd Kögler, Jürgen Lipp, Manfred Strohrmann

Das Buch gibt einen allgemeinen und praxisorientierten Überblick über die Anforderungen und Herausforderungen des Qualitätsmanagements – ergänzt um Aspekte der digitalen Transformation.

Es ist verständlich und anschaulich geschrieben und als Nachschlagewerk bei der Implementierung und Weiterentwicklung eines Qualitätsmanagementsystems gut geeignet. Insgesamt vermittelt das Buch Strukturen, Verfahren und Prozesse für die erfolgreiche Umsetzung eines Qualitätsmanagementsystems. Dabei werden auch Methoden- und Managementkompetenzen zur Gestaltung eines effektiven Qualitätsmanagementsystems vermittelt. Das Buch greift das Thema „Digitale Transformation" aus verschiedenen Blickwinkeln auf.

Das Kapitel „Qualitätsgesicherte Innovationen" gibt einen Einblick in unternehmerische Strukturen und Methoden. Hilfreich ist Kapitel 5. Auch wenn der Titel „Die Kunst, die richtigen Daten zu nutzen" beim Leser eine falsche Erwartungshaltung wecken kann, wird die Bedeutung der Datenqualität und des Datenmanagements gut herausgearbeitet.

Kapitel 8 ist den Prozessen gewidmet, deren Verbesserung und der Vorgehensweise bei der Digitalisierung, was durch die Kapitel 9 und 10 mit der Infrastruktur sowie „Digitale Kompetenz erwerben" abgerundet wird.

Das Literaturverzeichnis ist sehr umfangreich, ebenso wie das Stichwortverzeichnis, das die Suche nach Begriffen sehr erleichtert – was das Buch auch zu einem Nachschlagewerk für die tägliche Arbeit macht. Nicht zu vergessen das Glossar. Kapitel 12.1 - 12.3 mit Erläuterungen der Sprache und Abkürzungen des Qualitätsmanagers, des Datenanalytikers und des Dateningenieurs.

Gernot Freisinger, Oliver Jöbstl, Bernd Kögler, Jürgen Lipp, Manfred Strohrmann
DIE DIGITALE TRANSFORMATION DES QUALITÄTSMANAGEMENTS

Carl Hanser Verlag GmbH & Co. KG

2022
406 Seiten
Hard Cover, 49,99 Euro
ISBN 978-3-446-46884-9

Das Autorenteam besteht aus erfahrenen Experten aus Praxis und Wissenschaft aus unterschiedlichen Branchen.

Fazit:

Das Buch gibt einen allgemeinen und praxisorientierten Überblick über die Anforderungen und Herausforderungen des Qualitätsmanagements – ergänzt um Aspekte der digitalen Transformation. Das Buch ist verständlich und anschaulich geschrieben, praxisorientiert und als Nachschlagewerk bei der Implementierung und Weiterentwicklung eines Qualitätsmanagementsystems gut geeignet. Die Autoren verwenden die Wir-Form, was beim Lesen stört und für ein Fachbuch eigentlich nicht angemessen ist.

Rezensionen von

Regina Mühlich (CIPM)
ist Wirtschaftsjuristin und Geschäftsführerin der AdOrga Solutions GmbH. Sie ist Vorständin des BvD e.V., Mitglied im Ausschuss Recht & Politik sowie Leiterin des Committee Law & Politics des EFDPO.

▶ AdOrgaSolutions.de

ENTZAUBERUNG DES RECHTS AUF INFORMATIONELLE SELBSTBESTIMMUNG

Svenja Behrendt

Der Titel des Werkes ist Provokation, Herausforderung und Genuss zugleich. Ist doch das (Grund-) Recht auf informationelle Selbstbestimmung das Mantra im deutsche Datenschutzrecht. Umso mehrweckt das als Dissertation verfasste Werk die Neugier auf eine fachlich fundierte Auseinandersetzung mit diesem „Schlachtruf" der deutschen Datenschutzszene. Wer sich Handlungsempfehlungen für den Alltag als Datenschutzbeauftragte:r erhofft, wird enttäuscht. Dies war nie Ziel des Werkes. Wer jedoch eine grundlegende juristische Befassung schätzt und sich für Hintergründe interessiert, wird nicht enttäuscht werden. Ist das Recht auf informationelle Selbstbestimmung grundrechtsdogmatisch und grundrechtstheoretisch begründbar?

Die Autorin verneint dies im Ergebnis. An einem einfachen Beispiel in Bezug auf die Selbstbestimmung der eigenen Daten in der analogen Welt, dass es dadurch einen Anspruch auf Unterlassen der eigenen Wahrnehmung der eigenen Person gäbe, demonstriert sie die grundrechtsdogmatische Unbegründbarkeit.

Zuvor befasst sie sich mit den Anforderungen an ein Grundrecht, dass jedem zusteht und gegenüber jedem wirkt und dass somit jegliche Fähigkeit der Wahrnehmung anderer einen Angriff auf eben dieses Recht darstelle. Dabei legt sie auch dar, dass sich ein Großteil der derzeitigen Verarbeitungsbefugnisse auf Einwilligungen begründen, deren umfassende Rechtskonformität sie in Frage stellt. Hier regt sie eine Neuorientierung an, die ein Umdenken weg von der bisherigen Vorgabe erfordert. Sie sieht dabei auch die grundrechtsrelevanten technischen Entwicklungen als Chance, hier eine Neujustierung durchzuführen. Die Gedanken und Ausführungen sind auch vor dem Hintergrund interessant, dass die Konzeption und Begrifflichkeit der „informationellen Selbstbestimmung" innerhalb der Datenschutz-Grundverordnung nicht einmal in den Erwägungsgründen Eingang gefunden haben. Für das Verständnis, aber auch für die Weiterentwicklung des Datenschutzrechts eine Erkenntnis, die Berücksichtigung finden sollte.

Auch wenn nicht jeder Schlussfolgerung gefolgt werden muss, bringt dieses Werk viele rechtsdogmatisch hergeleitete Aussagen, die Datenschutzbeauftragten zwar nicht unmittelbar im Alltag helfen, bezüglich derer es aber wünschenswert ist, dass Überlegung bei der Einordnung und Fortentwicklung des Rechts in künftigen Erwägungen Eingang finden.

Svenja Behrendt
ENTZAUBERUNG DES RECHTS AUF INFORMATIONELLE SELBSTBESTIMMUNG

Verlag: Mohr Siebeck

1. Auflage 2023
430 Seiten
Preis 119,00 Euro
ISBN 978-3-16-161438-5

Rezension von

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

Anzeige

Jetzt 3 Monate ZD kostenlos testen.

ZD – Zeitschrift für Datenschutz

13. Jahrgang. 2023. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 319,–
Vorzugspreis für BvD-Mitglieder, für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 245,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 17,– 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. | 173613
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

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:

07.08.2023	RG Schwäbisch Gmünd	**27.10.2023**	RG Nürnberg
28.08.2023	RG West	**27.10.2023**	RG Schwäbisch Gmünd
04.09.2023	RG Schwäbisch Gmünd	**07.11.2023**	RG West
07.09.2023	RG Gütersloh	**15.11.2023**	RG Sachsen
12.09.2023	RG Sachsen	**30.11.2023**	RG Nord
29.09.2023	RG Stuttgart	**30.11.2023**	RG Gütersloh
02.10.2023	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 Know-how 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:

onetrust
▶ onetrust.de

RHENUS OFFICE SYSTEMS
▶ rhenus.group/de

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
Jetzt bewerben!
Einsendeschluss 06.12.2023
datenschutzmedienpreis.de
DAME 2023 DATENSCHUTZ MEDIENPREIS

Schulprojekt

Datenschutz geht zur Schule BvD e.V. DATENSCHUTZ GESTALTEN
"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 POWERED BY BvD
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

BvD-Fortbildungen

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Termin	Thema
17.08.2023	**Webinar – Prüfung von Auskunftsverlangen nach dem TTDSG über Bestands- und Nutzungsdaten: Eine (neue) Aufgabe für den DSB!**
07.09.2023	**Online-Seminar: Datenschutz-Managementsystem**
11.09.2023	**Webinar: Datenschutzschulung & Mitarbeitersensibilisierung**
14.09.2023	**Webinar – Datenschutz & Cloud – So bewerten Sie den Einsatz von Cloud Services**
19.09.2023	**Webinar – Datenschutz im Call-Center**
21.09.2023	**Präsenz-Seminar – Interne Ermittlungen unter Datenschutzgesichtspunkten** in Frankfurt/Main
28.09.2023	**Webinar – Sicherheit der Verarbeitung nach Art. 32 DS-GVO: Keine Verarbeitung ohne Rechtsgrundlage und Datenschutzhinweis**
13.10.2023	**Webinar: Löschung & DIN 66398 / DIN 32757**
26.10.2023	**Webinar – Datenschutzpannen: Was müssen Sie tun? Welche Risiken bestehen?**
07.11. - 08.11.2023	**Online-Seminar: Office 365 – Möglichkeiten und Risiken der Software**
08.11. - 10.11.2023	**Online-Seminar – Get Ready: Datenschutz für Koordinatoren**
16.11.2023	**Webinar – Hinweisgeberschutzgesetz (HinSchG) – Der externe DSB als Meldestelle**
28.11. - 29.11.2023	**Online-Seminar & Workshop – IT für Datenschutzbeauftragte**

JETZT ANMELDEN:
bvdnet.de/termine

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.

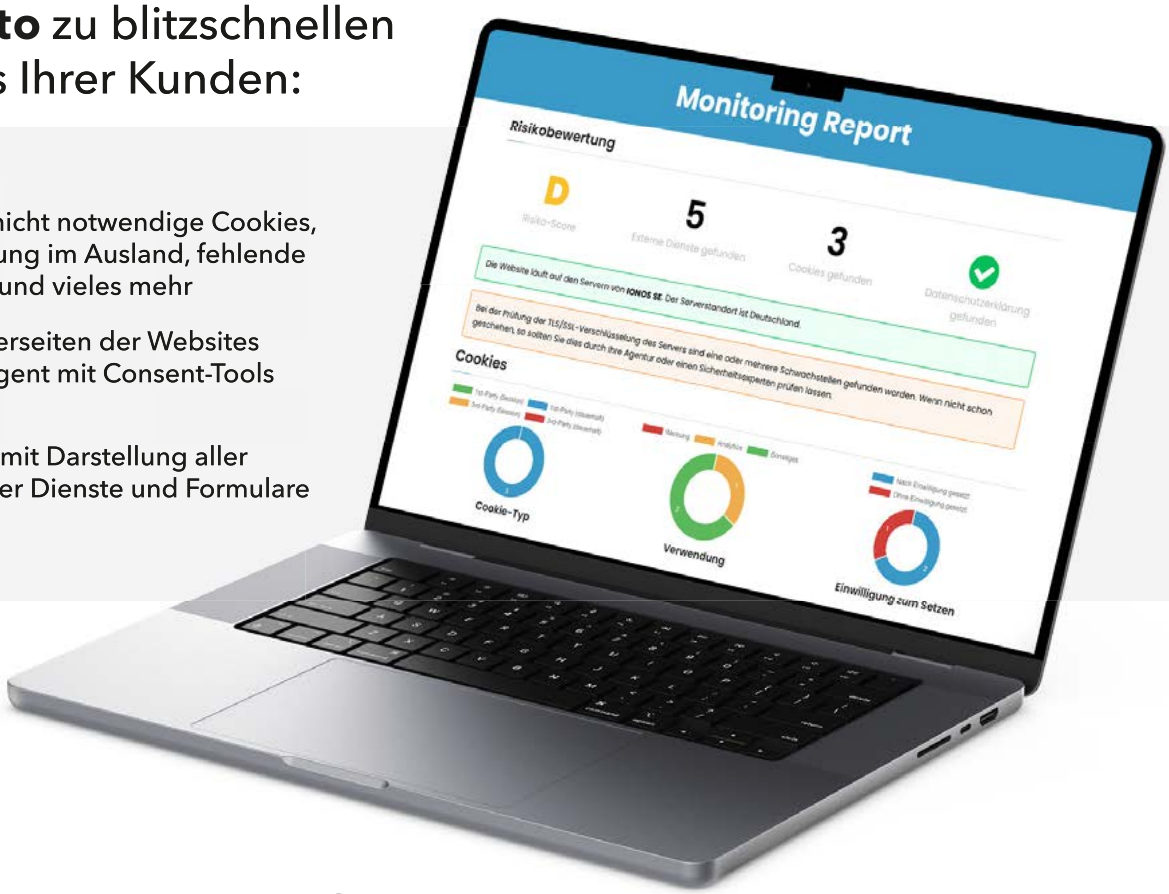
Der DSGVO-GUARD® ist ein Service der Website-Check GmbH - Beethovenstrasse 24, 66111 Saarbrücken

Anzeige

Websites manuell auf Datenschutzlücken zu durchsuchen ist Vergangenheit!

Mit **decareto** zu blitzschnellen DSGVO-Scans Ihrer Kunden:

- decareto prüft nicht notwendige Cookies, Datenverarbeitung im Ausland, fehlende Einwilligungen und vieles mehr
- durchsucht Unterseiten der Websites und geht intelligent mit Consent-Tools um
- erstellt Reports mit Darstellung aller Cookies, externer Dienste und Formulare



Sind Sie bereit dafür, Ihre Zeit besser zu nutzen?

- Mit dem **Report in Ihrem eigenen Branding** können Sie Ihrer Prüfpflicht nachkommen und Ihren Kunden fachliche Kompetenz demonstrieren.
- Unser DSGVO-Scanner erledigt zeitaufwändige Website-Prüfungen, damit Sie **Freiraum für anspruchsvollere Arbeiten** haben.
- Unsere Website-Überwachung schützt Ihre Kunden vor Abmahnungen und Bußgeldern und **stärkt damit Ihre Kundenbindung**.
- Prüfen Sie ohne viel Aufwand potentielle Neukunden auf Datenschutzlücken und erhöhen Sie Ihre **Akquise-Power**.

decareto

Alle Informationen finden Sie auf **www.decareto.de**
Vereinbaren Sie noch heute einen **Beratungstermin** unter **decareto.de/demo** oder besuchen Sie unsere Website für eine kostenfreie **14-Tage-Testphase.**