Ausgabe 03/2023

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

mastodon.social/@bvd@privacyofficers.social

linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD e.V.
DATENSCHUTZ GESTALTEN

2024

SAVE THE DATE

Jetzt Termine vormerken.

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

BVD-KONGRESSE 2024

BvD-Verbandstage
28.05. – 29.05.2024 in Berlin

3. Datenschutztag Hessen & Rheinland-Pfalz
25.06.2024 in Frankfurt/Main

BvD-Herbstkonferenz & Behördentag
16.10. – 18.10.2024 in Stuttgart

JETZT ANMELDEN:
bvdnet.de/termine

BvD e.V.
DATENSCHUTZ GESTALTEN

Liebe Leserinnen und Leser,

Bullshit-Bingo & Datenschutz – Wie passt das zusammen? Nun, jeder von uns kennt die typischen Modeworte der Beraterbranche, die dann alle sinnlos aneinander gereiht zum Bullshit-Bingo vermengt werden. Manchmal kommt es einem fast wie ein Wettstreit um die absurdesten Formulierungen vor.

Auch in der Datenschutzberatung – erlauben Sie mir diese selbstkritische Beobachtung – verbreitet sich dieses Phänomen zunehmend. Je intensiver sich Fachleute mit einem Datenschutzthema befassen, desto unverständlicher wird oft der Output.

Es ist ein Naturgesetz, dass immer noch ungeahnte Nebenthemen und Fragen aufkommen, wenn man nur tief genug in ein Thema einsteigt. Unser Fachgebiet nimmt ja auch zusehends an Komplexität zu, man denke nur an die zahlreichen neuen Rechtsakte der europäischen Digitalgesetzgebung. Nur muss man gut abwägen, ob die Befassung mit noch der kleinsten Verästelung einer Detailfrage jemandem nützt. Das ein oder andere Mal ist der Nutzen für den Schutzzweck nur noch schwer erkennbar, vielmehr scheint allenfalls noch intellektuelle Stimulation oder der Aufbau von Reputation in der Szene im Vordergrund zu stehen.

Unser Grundsatz war immer: Datenschutz soll den Betroffenen dienen.

Lassen Sie uns diesen Grundsatz stets im Auge behalten! Das sage ich als überzeugter Datenschutzbeauftragter, der seit über zwanzig Jahren Unternehmen im Bereich Datenschutz berät. Wenn zwischen deren praktischem Alltag und dem angestrebten Schutzzweck einerseits und dem an manchen Stellen hohen Theoretisierungsgrad und den daraus folgenden Anforderungen eine zu hohe Diskrepanz entsteht, tun wir niemandem einen Gefallen: weder den Betroffenen, noch den Verantwortlichen.

Letzten Endes auch unserem Berufsstand nicht. In Interviews werde ich oft gefragt, ob derzeit nicht goldene Zeiten für uns wären, da immer mehr Beratungsbedarf entstünde. NEIN - wir möchten bei aller Beratung vor allem, dass unsere Kunden (in Wirtschaft und Behörden) erfolgreich arbeiten können. Ich möchte, dass Verantwortliche, die die Bedeutung des Themas grundsätzlich erkennen und gewillt sind, hier auch zu investieren, nicht durch vollkommen theoretische und überzogene Forderungen, die den Betroffenen gar nichts mehr bringen, abgeschreckt werden und entmutigt aufgeben. Wir als BvD haben daher pragmatische Vorschläge für die Evaluierung der DSGVO vorgelegt – auch wenn es im nächsten Jahr höchstwahrscheinlich zu keiner Anpassung kommen wird. Die Themen und die Bereitschaft zur Verbesserung müssen breit diskutiert werden. Einen ersten Aufschlag dazu haben wir im September mit einer politischen Diskussionsveranstaltung in Berlin gemacht (siehe Nachbericht S. 6) sowie mit einem Positionspapier (Dokumentation S. 10).

Wir Datenschützer tun gut daran, stets den Schutzzweck im Blick zu haben und dem Ansatz der DSGVO zu folgen, die den Datenschutz risikobasiert und prozessual geregelt sehen will. So lässt sich Komplexität reduzieren und die konkrete Umsetzung bei den Verantwortlichen vereinfachen. Hier sind wir als Übersetzer gefragt, die erklären, vermitteln, Verständnis schaffen. Das sollte eines unserer vornehmsten Ziele sein. Wenn die Verantwortlichen das Gefühl haben, am Ende des Weges ist etwas Sinnvolles und Machbares entstanden, dann haben wir auch den Betroffenen geholfen. Dann haben wir wirklich etwas gekonnt.

Auch bei unseren BvD-Veranstaltungen wie zuletzt bei der Herbstkonferenz in München (siehe Nachbericht S. 48) und natürlich in den unserer BvD-News ist diese Herangehensweise unser Bestreben: pragmatisch, am Bedarf ausgerichtet und die Arbeit des DSB unterstützend. Ich hoffe, dass die vorliegende Ausgabe diesem Anspruch wieder gerecht wird und Sie viele praktische Überlegungen mitnehmen können.

Ihr

Thomas Spaeing
BvD-Vorstandsvorsitzender

INHALTSVERZEICHNIS

IM FOKUS

DATENSCHUTZRECHT

DATENSCHUTZPRAXIS

AUFSICHTSBEHÖRDEN

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-Herbstkonferenz: Uli Schneider

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.

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

CHRISTINA DENZ

"GANZ PERFEKT IST SIE NOCH NICHT"

BvD und Stiftung Datenschutz diskutierten mit Fachleuten in Berlin über die geplante DSGVO-Evaluation 2024.

Auf dem Podium der DSGVO-Veranstaltung von BvD und Stiftung Datenschutz (von links: Rechtswissenschaftler Boris Paal, der Baden-Württembergische Datenschutzbeauftrage Tobias Keber, Stiftung-Datenschutz-Vorsitzender Frederick Richter sowie die MdBs Misbah Khan (Grüne) und Thomas Jarzombek CDU)

Die erste Evaluation der seit 2018 geltenden Datenschutzgrundverordnung war 2020 - „und ist eigentlich ausgefallen". BvD-Vorstandsvorsitzender Thomas Spaeing erinnert sich gut an das Corona-Jahr, in dem Brüssel mit halber Kraft fuhr. Die nächste Evaluation ist nun für 2024 geplant. „Ob diese stattfindet, wissen wir noch nicht", sagte Spaeing zum Auftakt der gemeinsamen Veranstaltung mit der Stiftung Datenschutz, die am 5. September in der Alten Münze in Berlin stattfand. Aber vieles sei dem BvD und der Stiftung Datenschutz wichtig, „so dass wir uns schnell einig waren, gemeinsam darüber zu sprechen." Denn auch wenn die DSGVO ein Meilenstein des Datenschutzes ist, „ganz perfekt ist sie noch nicht", sagte Spaeing.

Dem BvD geht es vor allem darum, dass die DSGVO so ausgestaltet wird, dass insbesondere kleine und mittelständische Unternehmen (KMU) von Verwaltungspflichten entlastet werden. Der BvD hat hierzu ein Positionspapier mit drei Kernpunkten verfasst: Er fordert, die DSGVO müsse die Querschnittskompetenzen von Datenschutzbeauftragten auch für KMU und Datensicherheit festschreiben, bürokratische Pflichten aus der DSGVO risikoabhängig definieren und die Hersteller von digitalen Lösungen und Leistungen in die datenschutzrechtliche Haftung nehmen. (siehe Positionspapier im Anschluss an diesen Beitrag).

Gleich zum Auftakt der Veranstaltung unterstrich Spaeing, was Datenschutzbeauftragte (DSB) in Unternehmen und Behörden leisteten. Durch interne Audits etwa überwachten sie die in einem Betrieb oder einer Verwaltung ergriffenen technisch-organisatorischen Maßnahmen. Dabei hätten sie auch die Datensicherheit im Auge, so dass Verantwortliche, nachbessern und Schwachstellen beseitigen könnten, sagte Spaeing. Datenschutzbeauftragte brächten eine Querschnittskompetenz mit, von der vor allem KMU profitieren. Denn die verfügten meist nicht über das erforderliche Datenschutz- und Datensicherheits-Knowhow. IT-Fachleute

seien außerdem schwer zu bekommen. „Und wer sich bewirbt, geht nicht ins Sauerland, sondern dahin wo was los ist“, sagte Spaeing.

Gleichsam sehen sich Datenschutzbeauftragte wie Verantwortliche einem bürokratischen Aufwand gegenüber. Transparenz- und Hinweispflichten, Verarbeitungsdokumentationen - das alles belastet laut Spaeing die Unternehmen. Deshalb bekräftigte er die Forderung, Ausnahmen von bestimmten Anforderungen beispielsweise für Selbständige und kleine Betriebe zu ermöglichen, „und die DSGVO nicht mit dem Gießkannenprinzip auf alle Unternehmen anzuwenden.“

Um das komplexe Zusammenspiel von DSGVO etwa mit dem Data Act und dem Data Government Act ging es in der anschließenden Podiumsdiskussion. Zwar sei die DSGVO ein Erfolgsmodell – darüber waren sich die Bundestagsabgeordneten Thomas Jarzombek (CDU) und Misbah Khan (Grüne) mit dem Rechtswissenschaftler Prof. Dr. Boris Paal und dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Prof. Dr. Tobias O. Keber einig. Darüber hinaus zeigten sich schnell Unterschiede.

Vor allem die unterschiedlichen Auslegungen in den Datenschutz-Aufsichtsbehörden der Länder und die teils widersprüchlichen Empfehlungen zur Nutzung von digitalen Anwendungen bei verschiedenen Einrichtungen stießen bei **Thomas Jarzombek** auf Kritik. Dies führe bei Unternehmen zu Unsicherheiten und zeige, dass die Abstimmungen über die Datenschutz-Konferenz von Bund und Ländern (DSK) nicht immer gut funktioniere.

Er unterstrich: „Datenschutz ist super wichtig, aber wir dürfen es nicht übertreiben.“ Es sei fraglich, ob es in allen Bundesländern eigene Landesdatenschutzbeauftragte bräuchte.

Jarzombek plädierte für ein bundeseinheitliches Gremium, das beispielsweise über konkrete Anwendungen und ihre Rechtmäßigkeit entscheidet. Ein ähnliches Modell sieht er auch auf europäischer Ebene.

Zudem kritisierte er, dass die Aufsichtsbehörden bei Ministerien und Schulen besonders hohe Datenschutzbestimmungen etwa bei Video-Konferenz-Systemen geltend machten. Im Bundestag aber würden Microsoft-Teams, Zoom und WebEx genutzt.

Tobias O. Keber, seit 1. Juli 2023 Datenschutzbeauftragter von Baden-Württemberg, verteidigte die „vertikale Gewaltenteilung“. Die unterschiedliche Auffassung der Landesdatenschutzbeauftragten beim Thema Microsoft 365 bezeichnete er als „Geburtsfehler“ der

Dr. Viviane Reding, EU-Kommissarin a.D.

DIE MUTTER DER DSGVO

Die frühere EU-Kommissarin Dr. Viviane Reding warnt davor, dass Europa beim Datenschutz zurückfällt.

Als EU-Kommissarin habe sie ihre Aufgabe stets darin gesehen, nach vorne zu schauen und die Stärke Europas herauszustreichen, erinnerte sich die Journalistin und langjährige Politikerin der christdemokratischen EVP-Fraktion im europäischen Parlament an die Ursprünge der DSGVO, die sie als damalige EU-Kommissarin für Justiz, Grundrechte und Bürgerschaft auf den Weg brachte.

Den Grundstein für die DSGVO legten laut Reding der Vertrag von Lissabon 2009 und die ebenfalls seit 2009 geltende EU-Grundrechtecharta. Beide Texte verwiesen auf das Recht auf digitale Selbstbestimmung als ein europäisches Menschenrecht.

Bei den ersten Plänen für ein europäisches Datenschutzrecht im Januar 2012 hätte die EU-Kommission vor allem die großen Tech-Konzerne aus Amerika vor Augen gehabt. „Das war das erste Mal, dass wir exteritorial gedacht haben, um unsere Bürger zu schützen“, sagte Reding und fügte hinzu: „Die Amerikaner haben das sofort verstanden.“ 80 Lobbyisten seien aus den USA angereist - und hätten am Ende verloren. „Aber nicht wegen uns, sondern wegen Edward Snowden“, der im Sommer 2013 die Überwachungspraktiken der US-Geheimdienste enthüllte. Reding ging davon aus, dass die DSGVO ein internationaler Erfolg werden könnte. „Aber dass es so schnell ging, das habe ich nicht erwartet“, räumte sie ein. Die DSGVO sei mittlerweile ein „Golden Standard“.

Zugleich warnte Reding davor, mit den weiteren EU-Acts könne ein „Riesendurcheinander“ entstehen. Die EU müsse jetzt handeln, denn die technologische Entwicklung stehe mit Künstlicher Intelligenz (KI) und Quantencomputern erst am Anfang. Wichtig sei es deshalb, eine Kohärenz zwischen den Datenschutz-Aufsichtsbehörden in den EU-Ländern hinzubekommen. Wenn dies misslinge, werde Europa zum „Standard Taker“ werden. „Und das will ich nicht. Ich will, dass Europa Standard Maker wird“, sagte Reding.

DSGVO-Auslegung. Betroffene Institutionen hätten aber durchaus bei ihrer zuständigen Behörde nachfragen können, wie es diese handhabt.

Schulen, Verwaltungen und auch der Bundestag müssten sich am Ende aber die Frage stellen, wie ernst es ihnen mit der digitalen Souveränität sei. „Wenn wir in Deutschland und Europa eine digitale Souveränität haben wollen, müssen wir nach Alternativen schauen", sagte Keber. Aus der Praxis-Anschauung heraus müsse er auch feststellen: „Die digitale Kompetenz, die haben wir nicht." So müssten sehr schnell „dicke Bretter" gebohrt werden, auch beispielsweise beim Thema Pseudonymisierung.

Jura-Professor **Boris Paal** verwies darauf, dass die neuen EU-Acts die Komplexität des Datenschutzes in Europa verstärken. „Wir müssen sehen, dass Datenschutz nicht zum Wettbewerbsnachteil gerät", mahnte er. Manche Start-Ups überlegten, ob sie sich tatsächlich in Europa oder doch besser im EU-Ausland gründeten. Paal geht nicht davon aus, dass es im Zuge der Evaluation zu einer DSGVO-Reform komme: „Deshalb müssen Lösungen im bestehenden System entwickelt werden", sagte er.

Grünen-Abgeordnete **Misbah Khan** sprach von einer „wunderbaren Digitalgesellschaft" in Deutschland. Vielen sei bewusst, dass Datenschutz die Menschen schütze. Das Thema müsse aber noch mehr in die Gesellschaft getragen werden. Dass die DSGVO Innovationen behindere, sieht Khan nicht. „Wenn man den Bedingungen folgt, kann man Daten nutzen", sagte sie.

Stiftung-Datenschutz-Vorstand Frederick Richter und BvD-Vorstandsvorsitzender Thomas Spaeing moderierten die Veranstaltung.

Wie komplex sich Datenschutz in der Praxis darstellt, darüber berichteten die externe Datenschutzbeauftragte Andrea Backer-Heuveldop von der ds² Unternehmensberatung, Judith Leschanz aus Österreich, Datenschutzbeauftragte der A1 Telekom Austria und Vize-Präsidentin der europäischen Dachvereinigung EFDPO sowie Dr. Simon Menke, der bei der Otto Grup Holding den Bereich Gewerblicher Rechtsschutz und Datenschutz Konzern leitet.

Andrea Backer-Heuveldop sprach von einem „Overkill" vor allem für kleine und mittlere Unternehmen. Es sei mitunter schwierig zu erklären, was tatsächlich für den Datenschutz in einem Unternehmen erforderlich ist. Auch sie teilte die Auffassung, dass die DSGVO als „Gold Standard" Wettbewerbsvorteile bringt. „Das ist aber kein Selbstläufer und nicht für jede Branche eins zu eins übertragbar", sagte sie. Da sei eine Abwägung beispielsweise beim Auskunftsrecht und den Dokumentationspflichten nötig. Und bei der Herstellerhaftung: Denn KMU müssten sich darauf verlassen können, dass sie die Produkte, die sie einkaufen, nicht noch selbst konfigurieren müssten, um sie DSGVO-konform zu machen, sagte Backer-Heuveldop.

Simon Menke kritisiert insbesondere Hinweise in der DSGVO auf ihr Zusammenspiel mit anderen Gesetzen, beispielsweise in Artikel 95. „Den versteht kein Mensch", sagte er. Da entstehe eine „Regulierung gegeneinander, die so nicht weitergehen kann". Teilweise könnten Unternehmen die Anforderungen rein technisch nicht erfüllen. So müsste die Otto Group über die Nutzerzahlen Auskunft erteilen. Das Unternehmen könne seine Nutzer aber nur identifizieren, wenn es deren IP-Adresse speichere. Und damit könne das Unternehmen personenbezogene Daten gar nicht anonymisieren. Zudem arbeiten manche Unternehmen mit Hunderten von Auftragsverarbeitern zusammen. Solche Systeme umzubauen, koste Millionen, sagte Menke.

Die Kosten zum DSGVO-konformen Umbau in Betrieben hält auch **Judith Leschanz** für hoch. Als Beispiel nannte sie die Einwilligungserklärung, die die DSGVO fordert. „Gelten die alten noch oder brauchen wir neue Formulare?" Da hätten manche Unternehmen „wirklich Geld in die Hand nehmen" müssen. Für Bürgerinnen und Bürger hätte die DSGVO nicht so viel verändert. Viele fühlten immer noch Machtlosigkeit gegenüber großen Firmen. Aber für Unternehmen machten die Regelungen der DSGVO einen großen Unterschied.

Leschanz verwies außerdem auf Probleme mit dem Auskunftsrecht von Betroffenen nach Art. 15 DSGVO. Manche Menschen, die mit einem Unternehmen nicht klarkämen, machten davon exzessiv, teils schikanös, Gebrauch. Während die großen US-Konzerne „auf Knopfdruck" Auskunft geben könnten, sei dies für KMU oft schwierig.

Zudem müssten Informations- und Transparenzpflichten vereinfacht werden. „Die liest sich ja kein Mensch mehr durch“, sagte Leschanz. Vielmehr sollten sie „wie eine Waschanleitung“ zu lesen sein.

Vom aktuellen Stand der geplanten BDSG-Novelle berichtete **Stefan Sobotta**, Leiter des Datenschutzreferats im Bundesministerium des Innern und für Heimat. Er berichtete, dass die Bundesregierung mit der Reform die Datenschutzkonferenz (DSK) aufwerten wolle. Dies sei mit Blick auf verfassungsrechtliche Regelungen zu den Bund-Länder-Abstimmungen eine Besonderheit und zeige die Wertschätzung des Gesetzgebers für die DSK. Ziel sei es, dass die DSK dauerhaft Bestand habe.

Nicht vorgesehen ist in dem Entwurf laut Sobotta, für die DSK eine Geschäftsstelle einzurichten. Der Bund habe keine ausdrückliche Gesetzgebungskompetenz für den Datenschutz. Wenn dies geändert werden solle, müsste es eine staatsvertragliche Regelung geben. Dies gelte auch für Überlegungen zu Daten im Gesundheitsbereich. „Auch da sind wir verfassungsrechtlich gebunden“, sagte Sobotta.

Datenschutz-Aktivist **Max Schrems** beendete die Veranstaltung mit einem Plädoyer für eine strengere Kontrolle der Aufsichtsbehörden in den EU-Mitgliedsstaaten. Er sieht die geplante Ergänzungsrichtlinie der EU-Kommission zur besseren Durchsetzbarkeit von Datenschutz in allen Mitgliedsstaaten skeptisch. „Was ist, wenn die Aufsichtsbehörden nicht zusammenarbeiten wollen“, fragte er. Innerhalb der EU-Mitgliedsstaaten hätten sich unterschiedliche Rechtskulturen entwickelt. Diese miteinander in Einklang zu bringen, werde Zeit kosten. Er tippt darauf, dass es noch zehn Jahre dauern werde, bis es Änderungen an der DSGVO geben wird.

Die Videos der Vorträge und weitere Informationen zur DSGVO-Evaluation finden Sie auf der Website dsgvo-2024.org.

Über den QR-Code gelangen Sie direkt zu den Videos.

Über die Autorin

Christina Denz

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

ZUM AKTUELLEN STAND DER DSGVO-ERGÄNZUNG

Karolina Mojzesowicz, Leiterin der Einheit Datenschutz bei der EU-Kommission, berichtete im Interview mit dem Vorstand der Stiftung Datenschutz, Frederick Richter, über den aktuellen Stand der geplanten DSGVO-Ergänzung. Diese will im Kern eine einheitlichere Auslegung der DSGVO in allen EU-Mitgliedsstaaten herstellen.

Die wirksame Durchsetzung des EU-Datenschutzes sei Voraussetzung für die DSGVO, sagte Mojzesowicz. Gesetze hätten nicht besoders viel Bedeutung, „wenn sie nicht effizient und effektiv durchgesetzt werden“. Die Ergänzung soll eine kohärente Auslegung der Verordnung gewährleisten.

Die EU-Kommission nahm laut Mojzesowicz die Ergänzung am 4. Juli 2023 an. Sie enthält ihr zufolge eine Liste von Vorschriften, die eine reibungslosere Abstimmung unterstützen sollen. Dazu gehört eine Harmonisierung der Rechte der Beschwerdeführer. Mojzesowicz will diese europaweit vereinheitlichen, wenn eine Beschwerde ganz oder in Teilen von den nationalen Behörden zurückgewiesen wird.

Eine weitere Harmonisierung betrifft laut Mojzesowicz die bislang unterschiedlichen Praxisverfahren, wenn es von Seiten der Aufsichtsbehörden Untersuchungen bei Veranwortlichen oder Auftragsverarbeitern gibt. Danach soll die Partei, gegen die ein Verfahren eröffnet wird, das Recht erhalten, in wichtigen Phasen des Verfahrens gehört zu werden.

Zudem sehe die Ergänzung ein Recht auf Akteneinsicht währen der Phase der Streitbeilegung vor. Aber auch gemeinsame Untersuchungen und Amtshilfen regele die Ergänzung.

Zugleich machte Mojzesowicz deutlich, dass es bei der DSGVO „keine Änderungen im Allgemeinen“ gebe. Da die EU mittlerweile viele Gesetzte erlassen habe, die auf der DSGVO basierten, gebe es Bedenken, die DSGVO jetzt zu ändern.

DOKUMENTATION: DSGVO-EVALUATION 2024

Positionspapier des BvD

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in allen EU- und EWR-Mitgliedsstaaten verbindliches Recht. Ein wichtiger und richtiger Schritt! Datenschutz steht für Vertrauen und wird für viele Unternehmen zum Wettbewerbsvorteil.

Anlässlich der anstehenden zweiten Evaluierung der DSGVO in 2024 zeigt der BvD in diesem Papier auf, wie aus der Sicht der Datenschutzpraktiker die Wirtschaft – insbesondere auch kleine und mittelständische Unternehmen (KMU) – bei der Erfüllung datenschutzrechtlicher Anforderungen im Kontext zunehmender Digitalisierung noch besser unterstützt werden können.

1. Querschnittskompetenz von Datenschutzbeauftragten auch für bessere Datensicherheit nutzen – insbesondere in KMU

Betriebliche und behördliche Datenschutzbeauftragte (DSB) sind in Deutschland inzwischen seit mehr als einem halben Jahrhundert im Datenschutzrecht fest verankert. Sie sind für Verantwortliche in öffentlichen und nicht-öffentlichen Stellen mit ihrer Expertise die tragende Säule, auf die diese bauen können, um die mit den Geschäftsprozessen einhergehende Verarbeitung von personenbezogenen Daten von Anfang bis Ende (Datenlebenszyklus) gesetzeskonform und unter Wahrung der Rechte der betroffenen Personen zu planen und durchzuführen.

In Zeiten akuter Ransomware-, Hacking- und Cyberangriffe sowie Leaks und sonstiger digital geführter Angriffe auf öffentliche wie auch nicht-öffentliche Stellen ist die Pflicht zur Benennung von Datenschutzbeauftragten ein wichtiges Instrument zum Schutz personenbezogener Daten von Bürgern, da die Datenschutzbeauftragten auch Beratungsfunktionen hinsichtlich der Sicherheit der Verarbeitung der personenbezogenen Daten der unterschiedlichen Betroffenenkreise übernehmen. Durch interne Audits können Datenschutzbeauftragte die Wirksamkeit der ergriffenen Schutzmaßnahmen auch überwachen und auch auf Verbesserungen hinwirken. Insbesondere in kleinen und mittleren Unternehmen (KMU) stellt die Vielseitigkeit von Datenschutzbeauftragten, welche sich aus den fachlichen Anforderungen an die Qualifizierung für diese Rolle ergibt, einen Vorteil für die Unterstützung der Unternehmensleitung dar. Ohne diese Querschnittskompetenz der gerade auch bei KMU tätigen Datenschutzbeauftragten droht durch erfolgreiche Angriffe auf die Sicherheit der Verarbeitung gesamtwirtschaftlich beträchtlicher Schaden. Denn gerade bei KMU, welche sich nicht immer mehrere verschiedene Fachberater „einkaufen" können, stellt die nur für den DSB vorgesehene themenübergreifende Fachkompetenz eine Kostenersparnis dar.

DSB sind Teil der Lösung, nicht des Problems

Unabhängig davon, ob ein Datenschutzbeauftragter benannt ist, legt die DSGVO den Unternehmen, Behörden und sonstigen Stellen insbesondere mit den DSGVO-Artikeln 5, 24 und 32 Pflichten für die Verarbeitung personenbezogener Daten auf. Die Verantwortlichen sind gefordert, sowohl präventiv geeignete technische und organisatorische Maßnahmen (TOMs) umzusetzen, als auch reaktiv diese zu prüfen und zu aktualisieren. Dazu bedarf es einer den Anforderungen entsprechenden Expertise und Erfahrung innerhalb der Organisation, die sich in der Querschnittskompetenz der Datenschutzbeauftragten manifestiert.

Datenschutzbeauftragte sind damit das Messwerkzeug im Werkzeugkoffer der internen Selbstkontrolle für Unternehmen, Behörden und sonstigen Stellen. Sie schützen diese vor dem Risiko erst durch die ggf. sanktionsbewährte behördliche Kontrolle der zuständigen Aufsichtsbehörde auf Mängel und Fehler in der Umsetzung des Datenschutzrechts hingewiesen zu werden. Gleichzeitig begrenzen die Datenschutzbeauftragten durch ihre Beratung zu erforderlichen und angemessenen Schutzmaßnahmen die Beeinträchtigung durch Störungen der IT – sowohl von innen als auch von außen. Datenschutzbeauftragte geben bei der Wahrnehmung ihrer gesetzlichen Aufgaben – also insbesondere der Unterrichtung und Beratung der obersten Managementebene – wertvolle Impulse für die kontinuierliche Verbesserung der gesetzlich geforderten Datenschutzmaßnahmen, aber auch zur Angemessenheit dieser Maßnahmen. Mit ihrer Zuständigkeit für alle Fachbereiche, in denen Beschäftigte und Auftragsverarbeiter personenbezogene Daten verarbeiten, sind sie das Bindeglied, das die Einhaltung der Strategien zum Schutz personenbezogener Daten sowie der Datenschutzvorschriften überwacht und Beschäftigte und Auftragsverarbeiter zur Einhaltung der Vorgaben der Leitung berät.

Im Hinblick auf die ständig an Bedeutung zunehmenden Digitalisierungsvorhaben sind die Datenschutzbeauftragten unverzichtbare Berater und Unterstützer für die Rechtmäßigkeit der geplanten Vorhaben. Dabei fließt ihre Beratung bei frühzeitiger und ordnungsgemäßer Einbeziehung sowohl präventiv in die Planung der datenschutzkonformen Verarbeitung ein, als auch reaktiv bei der Behebung von Versäumnissen.

2. Bürokratische Pflichten zum Schutz personenbezogener Daten risikoangemessen ausgestalten

Die DSGVO weist eine ausgeprägte Compliance-Methodik aus, die sich darin niederschlägt, dass jede Zulässigkeitsbewertung durch Dokumentations- und Hinweispflichten und jede Handlungspflicht durch Organisationspflichten flankiert wird.

Die Frage nach der Zulässigkeit einer Verarbeitung gemäß Art. 6 DSGVO wird beispielsweise durch die Dokumentation nach Art. 5 Abs. 2 DSGVO (sog. Rechenschaftspflicht) und durch die Pflicht, gegenüber der betroffenen Person die Rechtsgrundlage nach Artt. 13, 14 DSGVO zu benennen, sowie durch die Pflicht zur Erfassung dieser Verarbeitungstätigkeit im Rahmen des Verzeichnisses von Verarbeitungstätigkeiten nach Art. 30 DSGVO flankiert. Damit löst selbst eine einfache Zulässigkeitsbewertung (z.B. die Verarbeitung der Kontodaten eines Beschäftigten zur Gehaltszahlung) drei weitere Pflichten aus. Hinzu kommt, dass diese flankierten Pflichten nicht harmonisiert sind, sondern jeweils eine eigene Ausprägung hinsichtlich des Was und Wie der Dokumentation bedeuten.

Jedes Unternehmen muss die Transparenz in Bezug auf die Verarbeitung personenbezogener Daten sicherstellen. Das bedeutet, dass die betroffene Person proaktiv umfassend über die Verarbeitung personenbezogener Daten informiert und ihr auf Verlangen reaktiv Auskunft erteilt werden muss. Nach der DSGVO müssen diese Pflichten jedoch nicht nur erfüllt werden, sondern nach Art. 5 Abs. 2 i.V.m. Abs. 1 lit. a DSGVO muss auch dokumentiert werden, dass diese Pflichten erfüllt werden, und nach Art. 12 DSGVO müssen – unabhängig von der Unternehmensgröße – nachweislich TOMs umgesetzt werden, um diese Transparenzpflichten zu erfüllen.

Festzustellen ist: Der eigentliche bürokratische und kostenintensive Aufwand durch die DSGVO besteht zum großen Teil darin, dass auch einfach zu bewertende und in jedem Unternehmen vorkommende Verarbeitungen personenbezogener Daten mehrere weitere Pflichten und Arbeitsaufwände auslösen.

Bürokratieentlastung von KMU: Vermeidung des Gießkannenprinzips

Es ist nicht so, dass diese zusätzlichen Aufwände unvermeidbar sind. Das vor der DSGVO geltende Bundesdatenschutzgesetz (BDSG) stellte in Bezug auf die Frage nach der (Un-)Zulässigkeit der Verarbeitung personenbezogener Daten keinen geringeren Schutz dar und kam dennoch ohne diese zusätzlichen Pflichten aus. Es lag damit in der Verantwortung des datenverarbeitenden Unternehmens, in Abhängigkeit von seiner Größe und des Risikos der ausgeführten Verarbeitung personenbezogener Daten entsprechende Vorkehrungen zu treffen.

Eine Änderung der Pflicht zur Benennung eines Datenschutzbeauftragten würde an dieser Bürokratie nichts ändern. Diese bußgeldbewehrten und auch zu Schadensersatzansprüchen führenden Pflichten müssen in jedem Fall erfüllt werden. In der Verantwortung hierfür steht die jeweilige Unternehmensleitung. Ohne Datenschutzbeauftragten fehlt der Unternehmensleitung jedoch der „Kompass“ durch die Bürokratie.

Ein wesentlicher Schritt zur Entlastung gerade von KMU besteht daher darin den die eigentlichen Kernpflichten der DSGVO überladenden Bürokratieüberbau abzubauen und solche Pflichten nur risikoangemessen vorzusehen und sie nicht – ausgehend vom höchsten Absicherungsbedürfnis – nach dem Gießkannenprinzip auf alle Unternehmen anzuwenden. Gerade wenn die Umsetzung der Anforderungen am Risiko für die Rechte und Freiheiten der betroffenen Personen ausgerichtet wird, können Datenschutzbeauftragte den geeigneten „Kompass“ darstellen.

3. Hersteller von digitalen Lösungen und Leistungen nach dem Verursacherprinzip in die Regelungen der DSGVO aufnehmen

Eine – wenn nicht sogar die – wesentliche Herausforderung für Anwender von Produkten zur Digitalisierung des Unternehmensalltags (seien es Applikationen, seien es andere digitale Lösungen und Leistungen) besteht darin, dass die Hersteller durch die DSGVO nicht direkt in die Pflicht genommen sind. Die Bewertung der datenschutzrechtlichen Anforderungen bleibt damit in der Verantwortung der Anwender hängen, obgleich sie IT-seitig davon ausgehen „Plug&Play“-Anwendungen zu kaufen. Der DSB ist dabei vielfach der Bote, der die schlechte Nachricht der fehlenden Erfüllung gesetzlicher Anforderungen überbringt. Ein wesentlicher Ansatz zur Entlastung der KMU besteht deshalb darin die Hersteller mit in die Pflicht zu nehmen. Die KMU müssen dann nur noch den konkreten Einsatz in ihrem unternehmerischen Umfeld prüfen.

Die Binsenweisheit, dass ein Problem dort gelöst werden muss, wo es entsteht, hat die DSGVO mit Art. 25 DSGVO versäumt umzusetzen. Denn wenn der Hersteller nicht bereits bei der Entwicklung und Herstellung des Produkts die Anforderungen des Datenschutzrechts umsetzt, kann der Anwender die Vorgaben der DSGVO mit einer solchen Anwendung auch nicht erfüllen.

Veranschaulichen lässt sich das anhand von Art. 25 Abs. 2 DSGVO: In der Praxis kann es sich für einen Verantwortlichen mitunter als schwierig erweisen, der Verpflichtung zur Ergreifung geeigneter technischer und organisatorischer Maßnahmen nachzukommen. Häufig wird er nämlich gar nicht in der Lage sein, sinnvolle und ausreichende TOMs zu implementieren. Denn sowohl die dafür verwendete Hardware als auch, noch bedeutsamer, die Software werden zumeist durch einen externen Hersteller und nicht den Verantwortlichen selbst bereitgestellt. Die TOMs, die der Verantwortliche beeinflussen kann, beschränken sich vielfach lediglich auf diejenigen Konfigurationen, die der Hersteller dem Verwender seiner Software, dem verantwortlichen Unternehmen, freiwillig ermöglicht. Bezüglich dieser Konfigurationen gilt dann natürlich uneingeschränkt die Pflicht aus Art. 25 Abs. 2 DSGVO, die datenschutzfreundlichsten zu wählen; insgesamt geht der Schutz personenbezogener Daten aber fehl.

Vorbild KI-Verordnung: Hersteller zu TOMs verpflichten

Trotz der offensichtlichen Einflussmöglichkeiten, die der Hersteller in Bezug auf die Ergreifung von insbesondere technischen Maßnahmen hat, welche er durch Voreinstellungen konfigurieren kann, lassen Wortlaut und Stellung der Norm im Kapitel „Verantwortlicher und Auftragsverarbeiter" keinen Zweifel daran, dass der Hersteller selbst nicht Adressat der Norm oder aus anderen Gründen zur Ergreifung von TOMs verpflichtet ist.

Um ein redaktionelles Versehen handelt es sich hierbei jedoch nicht. Denn der Hersteller findet durchaus Erwähnung. So ist im Satz 4 des Erwägungsgrundes 78 der DSGVO vorgesehen, dass Hersteller sicherstellen sollten, dass die Verantwortlichen und die Verarbeiter in der Lage sind, ihren Datenschutzpflichten nachzukommen. Zudem war ein entsprechender Vorschlag des Europäischen Datenschutzbeauftragten (EDSB), die Hersteller miteinzubeziehen, eben gerade nicht umgesetzt worden. Es besteht vor diesem Hintergrund daher eine Verantwortungs- und Haftungslücke, aufgrund derer die Effektivität des Art. 25 Abs. 2 DSGVO stark beeinträchtigt ist.

Nach dem Vorbild der anstehenden KI-Verordnung (Art. 24 des entsprechenden Kommissionsvorschlags) sollte auch im Bereich des Datenschutzrechts der Hersteller zur Ergreifung von TOMs verpflichtet werden. Damit würden die Datenschutzherausforderungen dort akkumuliert, wo sie entstehen – am Anfang der Kette. Dies würde es den Verantwortlichen erleichtern, ihrerseits der Pflicht, geeignete TOMs zu ergreifen, nachzukommen.

In Art. 25 DSGVO wäre ein zusätzlicher Absatz anzufügen, welcher die Verantwortung der Hersteller explizit regelt; idealerweise sollte hierbei die Einheit des Herstellerbegriffs mit dem der Produkthaftungsrichtlinie gewahrt werden. Dies könnte durch Einführung einer dahingehenden Definition in Art. 4 DSGVO garantiert werden (so bereits der Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DSGVO aus dem November 2019, S. 16 f.).

Die Erfahrungen der letzten Jahre haben gezeigt, dass es geboten ist, Art. 25 Abs. 2 DSGVO endlich zu einem wirksamen Instrument des Datenschutzes zu machen. Dafür ist es zwingend erforderlich, den Hersteller in den Adressatenkreis der Norm einzubeziehen und somit die heute bestehende Haftungslücke zu schließen. Dies würde gleichzeitig auch eine Inanspruchnahme des Herstellers nach Artt. 82 und 83 Abs. 4 lit. a) DSGVO ermöglichen.

DSGVO-EVALUATION 2020

Bereits anlässlich der ersten Evaluation der DSGVO 2020 hatte der BvD Vorschläge erarbeitet, wie Datenschutzbeauftragte insbesondere KMU noch effektiver unterstützen können. Über den QR-Code können Sie die Forderungen des BvD aus dem Jahr 2020 nachlesen.

Zum BvD-Positionspapier zur DSGVO-Evaluation 2020 gelangen Sie direkt über den QR-Code oder über die Website dsgvo-2024.org

NEUES ZU DEN EU DATA ACTS

Data Act und Data Governance Act: Funktioniert ein Datenrecht ohne Datenschutzrecht?

Kristina Schreiber

Zur Rolle des Datenschutzrechts in den neuen EU-Verordnungen zum Datenrecht

Die EU will die Datenwirtschaft beleben mit neuen Rechtsakten. Mit ihrer Digitalisierungsstrategie will sie bis 2025 eine effiziente, innovative und an den europäischen Werten, Grundrechten und Vorschriften ausgerichtete Datenwirtschaft aufbauen. Eine der tragenden Säulen dieser Strategie ist die sogenannte EU-Datenstrategie mit zwei neuen Rechtsakten: Dem seit September 2023 geltenden Data Governance Act (DGA) und der seit einigen Monaten bekannten Trilog-Fassung des Data Act (DA). Beide Rechtsakte – jeweils EU-Verordnungen – lassen die DSGVO unberührt und erwähnen sie doch gemeinsam fast 100 Mal. Dies verwundert nicht: Das Datenrecht regelt den Umgang mit Daten, auch mit personenbezogenen Daten. Das Datenschutzrecht wird damit von den Regelungen unmittelbar berührt, auch wenn die Rechtsakte selbst dies negieren wollen. Was also gilt in der Praxis und wie lässt sich eine Kongruenz herstellen zwischen Datenrecht und Datenschutzrecht?

Das Ziele der europäischen Datenstrategie

Eine florierende Datenwirtschaft im EU-Binnenmarkt ist das erklärte Ziel der EU. Zu erreichen versucht sie dieses Ziel mit einer Vielzahl neuer Rechtsakte, von der KI-Verordnung über Digital Markets Act und Digital Services Act bis hin zum Data Governance Act und dem Data Act. Die beiden letzten Rechtsakte sind Teil der sog. Datenstrategie, alle zusammen bilden sie – mit insgesamt knapp 50 weiteren Rechtsakten, die teils schon erlassen und teils noch zu entwerfen sind, die EU-Digitalstrategie. Die neuen „Acts" der EU ergehen überwiegend als EU-Verordnungen und sind damit unmittelbar anwendbar in den EU-Mitgliedstaaten. Die EU will die Unternehmen dabei stärken durch einen erleichterten Zugang zu Daten und die Förderung einer verantwortungsvollen Datennutzung. Ziel ist eine verbesserte Nutzung des Potentials der wachsenden Zahl vorhandener Daten für soziales und wirtschaftliches Wohlergehen.

Im Juni 2022 ist als erster Teil der EU-Datenstrategie der Data Governance Act (DGA) verkündet worden, an den sich Unternehmen und Behörden ab September 2023 halten müssen (Verordnung EU 2022/868). Im Juni 2023 konnte zudem im Trilog eine politische Einigung über den Data Act (DA) erzielt werden, dessen finaler Text voraussichtlich noch Ende des Jahres verabschiedet werden wird. Der DA ist der zweite Teil der EU-Datenstrategie.

Während sich der DGA vor allem mit der Weiterverwendung von Daten der öffentlichen Hand und unabhängigen beziehungsweise nicht-kommerziellen Verarbeitungsformen (Datenmittler, altruistische Datenorganisationen) beschäftigt, wird der DA in fast alle Bereiche der Datennutzung hineinwirken mit Regelungen unter anderem zum Zugang von Nutzungsdaten und Pflichten zur Datenportabilität, zur Missbrauchskontrolle von Verträgen über die Datennutzung, zu Datenübermittlungen in Drittstaaten, Interoperabilitätsvorgaben, Datenbereitstellung und Zugangsgewährung sowie einer Pflicht, Daten öffentlicher Stellen etwa in Notfallsituationen bereit zu stellen. Kurzum: Unter dem DA werden Anbieter von digitalen Produkten Nutzern automatisierten Zugang zu Metadaten gewähren müssen, die Migration zu anderen Diensten zu erleichtern haben und Verträge über die Datennutzung bei Beteiligung von kleinen und mittleren Unternehmen auf einen fairen Ausgleich hin zu überprüfen haben.

DGA, DA und der Datenschutz

All diese Daten, die über die Vorgaben in DGA und DA reguliert werden, können auch personenbezogene Daten i.S.d. Verordnung (EU) 2016/679, der DSGVO darstellen. DGA und DA gelten für nicht-personenbezogene Daten und personenbezogene Daten gleichermaßen.

Und dennoch lassen beide Rechtsakte nach ihrem jeweiligen Art. 1 Abs. 3 die DSGVO „unberührt":

Art. 1 Abs. 3 DA regelt, dass für personenbezogene Daten, die im Zusammenhang mit den Vorgaben des DA verarbeitet werden, die Rechtsvorschriften der Union und der Mitgliedstaaten über den Schutz personenbezogener Daten gelten. Die DSGVO bleibt unberührt, im Fall eines Widerspruchs zwischen DSGVO und DA soll die DSGVO Vorrang haben.

Art. 1 Abs. 3 DGA sieht dies ähnlich: Die DSGVO gilt für alle personenbezogenen Daten und der DGA gilt „unbeschadet" der DSGVO. Im Fall eines Konfliktes soll die DSGVO auch Vorrang vor dem DGA genießen.

Beide Rechtsakte stellen zudem klar, dass sie keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen, der DGA in Art. 1 Abs. 3 a.E., der DA in Erwägungsgrund 7.

Welcher Gehalt aber kommt diesen Regelungen zu, wenn beide EU-Verordnungen alleine den Umgang mit Daten, auch personenbezogenen Daten, regeln und gemeinsam beinahe 100 mal die DSGVO erwähnen? Kann so ein Rechtsakt „unberührt" bleiben? Um dies näher zu untersuchen, müssen wir zunächst einen genaueren Blick auf den Regelungsgegenstand von DGA und DA werfen.

Der Data Governance Act

Der DGA ist im Juni 2022 in Kraft getreten und gilt seit September 2023. Als EU-Verordnung gilt er unmittelbar in jedem Mitgliedsstaat, ohne dass es einer Umsetzung in nationales Recht bedarf. Dabei schreibt er sich große Ziele auf die Fahne: Der DGA soll die Hemmnisse für eine gut funktionierende Datenwirtschaft abbauen und einen EU-weiten Rechtsrahmen für den Zugang zu Daten und deren Verwendung schaffen.

Dies möchte der DGA dadurch bewerkstelligen, dass er eine Art Infrastruktur für den Datenmarkt bereitstellt. Anbieter sog. „Datenvermittlungsdienste" sollen als Mittler zwischen Dateninhabern und (potentiellen) Datennutzern das Teilen und die Nutzung von Daten fördern, dürfen in der Union aber nur tätig werden, wenn sie bestimmte formelle und materielle Voraussetzungen erfüllen und sich damit registrieren. Befinden sich Daten im Besitz öffentlicher Stellen, sollen diese als weitere Säule des DGA möglichst breit und diskriminierungsfrei der Öffentlichkeit zur Verfügung stehen. Darüber hinaus soll ein System für mehr Vertrauen in den „Datenaltruismus" geschaffen werden: Altruistische Organisationen können sich registrieren lassen und erhalten dann das Logo „Anerkannte altruistische Datenorganisation". Für diese wird die EU-Kommission auch ein Musterformular für eine Einwilligung bereitstellen.

Der Data Act

Seit Ende Februar 2022 liegt zudem der Entwurf des Data Act (DA) vor, seit Juli 2023 in einer informellen Fassung, die die im Trilog gefundene Einigung widerspiegelt (14.07.2023, Interinstitutioneller File Nr. 2022/0047 (COD)). Auch der DA beschäftigt sich mit einheitlichen Vorschriften für den fairen Zugang zu Daten und deren Nutzung in Form einer EU-Verordnung. Er enthält weitreichende Regelungen für die privatwirtschaftliche Datennutzung.

Der Fokus des DA liegt auf Industriedaten, Maschinendaten, deren Nutzung durch Rechtssicherheit erleichtert werden soll. Er erfasst aber ebenso personenbezogene Daten, etwa die Nutzungsdaten in einer jeden von Endverbrauchern verwendeten App. Der Abbau technischer Hindernisse soll den Weg zu einer interoperablen und agilen Datenwirtschaft ebnen. Damit steigt die EU erstmals in die Regulierung des eigentlichen Datengeschäfts ein. Zuvor waren Vorgaben oft auf Spezialbereiche beschränkt oder zielten auf konkrete marktstarke Player wie Amazon, Apple, Google oder Facebook (Meta) ab. Dazu kommen Regelungen zur Missbrauchskontrolle von Verträgen über die Datennutzung die mit anderen Unternehmen abgeschlossen werden, Datenübermittlungen in Drittstaaten, Pflichten zur Datenportabilität und einiges mehr. Der DA umfasst damit im Gegensatz zum DGA, der sich vor allem mit der Weiterverarbeitung von Daten der öffentlichen Hand, dem allgemeinen Rechtsahmen für Datenvermittlungsdienste und nicht-kommerziellen Verarbeitungsformen beschäftigt, fast alle Bereiche der Datennutzung. Auch der DA betrifft dabei personenbezogene und nicht-personenbezogene Daten.

Datenschutz im Datenrecht

Der Blick auf die Regelungsgegenstände von DGA und DA verdeutlichen denn auch unmittelbar, dass eine „Unberührtheit" der DSGVO illusorisch erscheint. Erwägungsgrund 7 DA offenbart denn auch das ganze Dilemma, wenn er einerseits konstatiert, dass die DSGVO unberührt bleibe und der DA keine Rechtsgrundlage für die Verarbeitung personenbezogener Daten bietet, dann aber andererseits konkret ausführt, dass der DA Dateninhabern unter bestimmten Voraussetzungen die Pflicht auferlegt, Daten – auch personenbezogene Daten – Dritten zur Verfügung zu stellen. Ist dies also eine unionsrechtliche Pflicht i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO, bestimmte

personenbezogene Daten zu verarbeiten? Streng genommen scheint die Vorgabe, die DSGVO bleibe „unberührt" dagegen zu sprechen. Erwägungsgrund 7 DA formuliert aber weiter, dass es von Interesse sein könnte, die Erfüllung der Anforderungen des Art. 6 DSGVO zu erleichtern. Was dies genau bedeutet, bleibt indes offen. Vorgeschlagen wird als Lösung in Erwägungsgrund 7 eine Anonymisierung der Daten, was sicherlich dem Datenschutz dient, indes keine Antwort auf die Frage nach der Erlaubnisgrundlage für die weitere Verarbeitung (und auch die Anonymisierung) gibt. Auch der DGA bringt eine Reihe ungeklärter Fragen mit sich: Datenvermittlungsdienste verarbeiten personenbezogene Daten, ohne dass dies nach dem DGA erlaubt sei. Sie benötigen nach der DGA-Konzeption hierfür eine gesonderte Erlaubnis nach den Vorgaben der DSGVO. Der EHDS, der European Health Data Space, soll dagegen in sich eine Erlaubnisgrundlage bringen. Für eine Förderung der rechtssicheren gemeinsamen Datenverarbeitung ist dies förderlich.

Sicher ist: DA und DGA führen in einer Vielzahl von Fällen zur Verarbeitung personenbezogener Daten, ja verpflichten insbesondere bei den Datenzugangs- und Datenbereitstellungspflichten im DA sogar dazu. Aber ob die Erfüllung dieser Pflichten dann auch datenschutzrechtlich erlaubt ist, bleibt offen.

Erlaubnisgrundlage nach DSGVO

Personenbezogene Daten dürfen verarbeitet werden, wenn die Verarbeitung „zur Erfüllung einer rechtlichen Verpflichtung erforderlich" ist (Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO). Stehen sensible Daten in Rede, zum Beispiel Gesundheitsdaten, dürfen diese verarbeitet werden, wenn ein Gesetz dies vorsieht, das „in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht" (Art. 9 Abs. 2 lit. j DSGVO).

Beide Vorschriften setzen allerdings eine tatsächliche Verpflichtung zur Datenverarbeitung voraus. Diese findet sich nicht, weder in DGA noch DA, denn dort heißt es jeweils ausdrücklich, dass diese Rechtsakte keine Erlaubnisgrundlage für die Verarbeitung personenbezogener Daten darbieten würden. Dann aber kann dieses Ergebnis auch nicht über eine Konstruktion erreicht werden, die Regelungen aus DGA und DA als rechtliche Verpflichtungen zur Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. c, Art. 9 Abs. 2 lit. j DSGVO einordnet. Eine entsprechende Erlaubnisgrundlage wird sich vielmehr aus anderen Regelungen ergeben müssen, insbesondere einer Einwilligung oder im Einzelfall womöglich auch den berechtigten Interessen der Dateninhaber und Datenempfänger (Art. 6 Abs. 1 UAbs. 1 lit. a, f, Art. 9 Abs. 2 lit. a DSGVO).

Datenverarbeitungsgrundsätze

Die Gestaltungsvorgaben des DA lassen auch den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO unberührt und sollen nicht als Verpflichtung zu verstehen sein, Produkte und damit verbundene Dienstleistungen so zu gestalten, dass sie personenbezogene Daten über das hinaus verarbeiten oder speichern, was für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Erwägungsgrund 19 DA). Diese simple Feststellung ist prima facie folgerichtig, zeigt bei genauerer Betrachtung indes erneut das volle Dilemma, das durch die Regelung verursacht wird, dass die DSGVO „unberührt" bleiben soll, obwohl der DA in umfangreicher Art die Datenverarbeitung reguliert. Denn wenn die Datennutzung gefördert werden soll, zugleich aber der Grundsatz der Datenminimierung ungeachtet der DA-Vorgaben zu bewerten ist, was gilt dann? Die Datennutzung ist zu minimieren. Aber ist das im Sinne des DA? Es entsteht ein Zielkonflikt, den der Verantwortliche, der Dateninhaber zu klären hat mit allen verbleibenden Rechtsunsicherheiten.

Datenrecht funktioniert nicht ohne Datenschutzrecht

Der politische Kompromiss war naheliegend: Die DSGVO ist lange verhandelt, jeder Berührungspunkt droht zu einem unlösbaren Konflikt zu werden. Das Ziel, DGA und DA möglichst schnell zu verabschieden, war daher am besten zu erreichen, wenn die DSGVO „nicht angefasst wird". Die Regulierung von Daten führt aber unweigerlich auch zu Regelungen über den Umgang mit personenbezogenen Daten. Rechtsdogmatisch mag dann die verordnungsrechtliche Vorgabe eines Vorrangs der DSGVO eine schematisch gute Lösung darstellen. Sie funktioniert aber nicht, weil das Datenschutzrecht unweigerlich berührt wird, und zwar an unzähligen Stellen und mit unzähligen Abwägungsfragen, die entschieden werden müssen: Wo verlangt der Datenschutz eine Beendigung und Einschränkung der Verarbeitung, wo soll zur Förderung der gemeinsamen Datennutzung oder der Datenwirtschaft die Verarbeitung gefördert werden? Dieses Dilemma hat der EU-Gesetzgeber den Anwendern aufgebürdet. Es ist an den Verantwortlichen, hier eine kongruente Lösung zu finden.

Über die Autorin

Dr. Kristina Schreiber
ist Rechtsanwältin, CIPP/E, Fachanwältin für Verwaltungsrecht und Partnerin bei Loschelder Rechtsanwälte in Köln. Sie ist spezialisiert auf die rechtliche Begleitung von Digitalisierungsprojekten und veröffentlichte den Praxisleitfaden „Digitale Angebote", außerdem einen Kommentar zum TTDSG und ist Mitverfasserin eines Einführungsbandes zum Data Governance Act, der demnächst um eine Einführung zum Data Act erweitert wird. Sie bloggt außerdem auf digitalisierungsrecht.eu

„DIE PSEUDONYMISIERUNG IST EINE FAULE AUSREDE“

Carl Fabian Lübke alias Flüpke ist IT Security Analyst. Als Hacker vom Chaos Computer Club spürt er Schwachstellen bei Firmen und Organisationen auf. Mit der BvD-News sprach Flüpke über Chancen und Gefahren der elektronischen Patientenakte (ePA).

BvD-News: *Herr Lüpke, die ePA ist lange geplant und immer noch nicht vollständig umgesetzt. Was ist der aktueller Stand?*

Carl Fabian Lüpke: Mittlerweile sind wir bei Stufe 5 angelangt, die erste Stufe war 2021 eingeführt worden. Mit jeder Stufe kamen mehr Features und Möglichkeiten hinzu. Beim Datenschutz hat sich allerdings keine weitere Verbesserung ergeben. Vielmehr haben sich weitere Datenschutzprobleme aufgetan und die sind bis heute nicht ausgeräumt.

BvD-News: *Welche sind das aus Ihrer Sicht?*

Carl Fabian Lüpke: Im Grunde handelt es sich bei der ePA um einen Cloud-Datenspeicher. Ärzte können dort Daten hineinspeichern und wir selbst können unsere Daten dann freigeben, das ist zumindest die Idee. Bislang folgten diese Daten keiner besonderen Struktur, es konnten in diesem Speicher PDF-Dateien oder Word-Dokumente stehen. Diese hat sich ein Arzt angeschaut und daraus Schlüsse gezogen. Mittlerweile geht es aber darum dort maschinenlesbare Formate zu hinterlegen, also medizinische Informationsobjekte, damit der Computer zum Beispiel eine Veränderung der Blutwerte erkennen kann.

Das würde medizinisch vielleicht Vorteile bringen, wenn Maschinen und Netzwerke die Entwicklung der Gesundheit über einen längeren Zeitraum erfassen, zum Beispiel die Veränderung des Gewichts einer Person. Daraus ließen sich sicher Vorhersagen treffen, welches Risiko sich aus diesen Daten für bestimmte Krankheiten ableiten lässt. Es wird also einfacher medizinische Daten zu verarbeiten. Und das wiederum sorgt dafür, dass mehr Unternehmen Software oder Apps anbieten, um diesen Krankheiten vorzubeugen. Damit aber steigt das Risiko für Missbrauch. In Finnland beispielsweise gab es 2020 einen Datenbreach bei einem Psychotherapiedienstanbieter. Dort wurde die komplette Patientendatenbank abgezogen und Namen und Befunde online gestellt. Das muss für die Betroffenen traumatisch gewesen sein. Wir brauchen also einen sicheren Zugang zur ePA.

BvD-News: *Warum hat das bislang nicht funktioniert?*

Carl Fabian Lüpke: Wir haben zwar in Deutschland eine hohe Awareness für Privacy und Datenschutz. Und man kann durchaus sichere Anwendungen bauen, die über einen geeigneten Datenschutz verfügen. Aber wir haben bislang noch kein einziges System gesehen, dass diese Standards erfüllt und man es als Opt-Out für die gesamte Bevölkerung ausrollen könnte. Es gibt einfach eine große Diskrepanz zwischen den Anforderungen an die Systeme und deren bisheriger Umsetzung.

BvD-News: *Ein Argument ist stets, dass die Gesundheitsdaten für die Forschung verwendet werden sollen. Wie kann das sicher und datenschutzkonform geschehen?*

Carl Fabian Lüpke: Die Versicherer bearbeiten Gesundheitsdaten schon jeher für unterschiedliche Zwecke, zum Bespiel für die Abrechnungen oder Statistiken über die Häufigkeit bestimmter Erkrankungen. Heikel wird es, wenn die Krankenkasse die Daten weitergibt. Oder wenn aus der ePA einzelne Daten weiterverarbeitet werden, die sich einer Person zuordnen lassen. Ich kann nicht beurteilen, wie wichtig solche Daten für die Medizinforschung sind. Bedenken muss man

aber, dass sich Fehler in diese Daten einschleichen können. Deshalb hat Gesundheitsminister Karl Lauterbach in seiner Digitalisierungs-Strategie darüber nachgedacht Dokumentationspflichten für Behandelnde festzuschreiben. Das kann auch für Patienten einen Mehrwert bedeuten, hätte aber zur Folge, dass dann wirklich alles über eine Person in der ePA stünde. Anders verhält es sich, wenn die Forschung mit relativierenden Daten arbeitet, also eine Anonymisierung vornimmt, bei der ein einzelner Datensatz nicht mehr einer Person zugeordnet werden kann. Das war ja beispielsweise bei den Coronastatistiken der Fall. Eine Pseudonymisierung, die von vielen favorisiert wird, halte ich dagegen für eine faule Ausrede. Man braucht ja wirklich nicht viele Daten, um einen Datensatz auf eine einzelne Person zurückführen zu können. Da reichen Geburtsdatum, Geschlecht und Geburtsort. Damit ist der Kreis schon sehr eingegrenzt. Kommt der aktuelle Wohnort dazu, ist die Person identifizierbar. Ich versehe, dass die Medizin den Verlauf von Krankheiten und Behandlungen erfassen will. Das geht nur, in dem man einzelne Personen betrachtet. Aus datenschutzrechtlicher Sicht allerdings lehne ich das ab.

BvD-News: *Und jetzt drängt zu all den Überlegungen noch KI hinzu. Welche Rolle kann sie im Gesundheitsbereich und bei der ePA spielen?*

Carl Fabian Lüpke: Ein mögliches Szenario wäre, dass die KI die in der ePa hinterlegten Dokumente scannt, die Daten daraus in einer standardisierten Form extrahiert und diese zum Beispiel an eine medizinische Auskunftei weitergibt. Da bleibt natürlich ebenfalls die Frage, was passiert, wenn ein Datenleck entsteht. Denkbar wäre auch, dass die KI aus den extrahierten Daten Schlussfolgerungen auf Krankheiten und Therapien zieht. Wenn der Computer aber eine falsche Entscheidung trifft, was dann? Die KI kann man nicht verantwortlich machen. Ist das Risiko kalkulierbar? Das ist alles unklar. Dann kommt ein oft diffuser Algorithmus hinzu. Als Security Analyst sehe ich, was bei Programmen und Anwendungen schief läuft, und kann dann sagen „Bitte ändern." Aber wenn etwas in einer KI abläuft, können wir nicht eingreifen. Wir können am Ende nicht mehr nachvollziehen, wo wann was schiefgelaufen ist. Und schließlich geht es immer wieder um die Frage um den Bias der Trainingsdaten. Von welchen Befunden, Krankheiten, Heilungen, von welchen gesellschaftlichen Gruppen und Geschlechtern werden da Daten eingespeist? Wenn wir Computer einsetzen, müssen wir sehen, dass wir Rassismus und Diskrimierungen überwinden. Das sehe ich aber noch nicht. Vielleicht darf ich die Frage umkehren: Würden Sie sich lieber von einer KI oder von einem Menschen diagnostizieren lassen?

BvD-News: *Blicken wir noch mal auf die digitalen Gesundheitsanwendungen. Wie sieht es denn bei denen mit Datenschutz aus?*

Carl Fabian Lüpke: Bei denen, die ja auch in die ePA integriert werden sollen, haben wir in der Vergangenheit teils gravierende Sicherheitslücken entdeckt. Die Idee ist es Startups sozusagen als Wirtschaftsförderung zu erleichtern an den Markt zu gehen. Aber so etwas macht man nicht mit Patientendaten, dass ist einfach komplett unverantwortlich. Denn es besteht ja die Gefahr, dass über die Apps Gesundheitsdaten abfließen.

Unklar ist meines Erachtens auch, was ist, wenn die App eine Krankheit ableitet und die dann über die ePA in den Algorithmus der Krankenkassen einfließt? Ein solcher Befund könnte dann auch noch eine oder zwei Generationen später treffen. Medizinische Daten haben eine zeitliche Relevanz weit über die Lebensdauer der Computersysteme, die sie verarbeiten und der Lebensdauer der Schutzmechanismen, die jetzt unsere Daten schützen, hinaus. Deshalb müssen wir sehr vorsichtig sein. Die Politik kann sich ändern, die wirtschaftlichen Bedingungen können sich ändern. Da könnten in einer anderen Generation die Daten sehr schnell gegen die Menschen verwendet werden.

BvD-News: *Das klingt nach einer Dystopie der Kontrolle über den Menschen.*

Carl Fabian Lüpke: Wir müssen da gar nicht so weit schauen. Es ist ja durchaus realistisch, dass wir eine Art Gesundheits-Schufa bekommen können. In Teilen haben wir das ja schon. Wer beispielsweise in eine Privatversicherung wechseln will oder eine Zusatzversicherung abschließt, wird nach seinen zu erwartenden Krankheiten taxiert.

Was ist, wenn allein diese Prüfung umgedreht wird nach dem Motto: Sie haben sich gefälligst gesund zu ernähren. Das hat Auswirkungen auf unsere persönlichen Freiheiten.

BvD-News: *Überhaupt gibt es ja auch bei der ePA Unterschiede zwischen Privat- und Kassenversicherten.*

Carl Fabian Lüpke: Bislang ist die Teilnahme der Privatkassen an der ePA freiwillig. Wohingegen die ePA für gesetzlich Versicherte über kurz oder lang zwangsweise eingeführt wird.

Privatsphäre ist also schon jetzt ein kostenpflichtiges Extra. Wenn ich zum Psychiater gehe und dort meine Gesundheitskarte abgebe, komme ich in der Regel nicht mehr in eine private Krankenversicherung wegen des erhöhten Risikos an einem psychischen Leiden zu erkranken. Gehe ich aber mit einem Batzen Geldscheine in die Praxis und bezahle, ohne dass ich die Gesundheitskarte nutze, hinterlässt die Behandlung keine Einträge im System. Das heißt: Privatsphäre kostet Geld. Und das darf eigentlich nicht so sein.

BvD-News: *Was schätzen Sie, wann es mit der ePA endlich soweit sein wird?*

Carl Fabian Lüpke: Nach den Verzögerungen in den vergangenen Jahren tue ich mich mit Prognosen mittlerweile schwer. Ich vermute aber, dass das e-Rezept recht zeitnah kommen wird.

Das Interview führte Christina Denz.

DR. FLORIAN EISENMENGER

EUROPÄISCHER DATENSCHUTZ VS. CHINESISCHE SICHERHEITSGESETZE

Ergebnisse eines Transfer Impact Assessments

Trotz des Inkrafttretens des EU-U.S. Data Privacy Frameworks am 10. Juli 2023 unterliegen internationale Datentransfers unverändert hohen datenschutzrechtlichen Hürden. Zwar lassen sich personenbezogene Daten auf dessen Grundlage (vorerst) wieder rechtssicher in die USA übermitteln. „Schrems II" [1] gilt allerdings nicht nur für die Übermittlung personenbezogener Daten in die USA, sondern für jedes Drittland ohne Angemessenheitsbeschluss. Angesichts dessen überrascht es, dass sich die Diskussion um die Zulässigkeit internationaler Datentransfers so stark auf die USA fokussiert.

Dieser Beitrag richtet den Blick daher auf die Volksrepublik (VR) China. In einem kurzen Überblick werden die Anforderungen an Transfer Impact Assessments (TIA) rekapituliert und am praktischen Beispiel eines für die VR China durchgeführten TIA illustriert.

Wann werden TIAs benötigt?

Internationale Datentransfers sind für viele Unternehmen die Regel. Typische Anlässe sind etwa die Zentralisierung von Softwaresystemen bei der US-Konzernmutter oder der Dienstleister, der nach dem follow-the-sun-Prinzip arbeitet und personenbezogene Daten in Indien, Singapur oder den USA verarbeitet. Auch der Einsatz von Unterauftragsverarbeitern in Drittländern mag in manchen Fällen ein TIA erforderlich machen. Die hohen Anforderungen an TIAs stellen viele Unternehmen vor Herausforderungen.

In Kürze: Anforderungen an TIAs und Drittlandbewertungen

TIAs sind grundsätzlich bei allen Datenübermittlungen auf Grundlage der Garantien des Art. 46 DS-GVO durchzuführen.[2] Sie sind gleichzeitig vertragliche Pflicht nach Klausel 14 der Standardvertragsklauseln.[3] Struktur, Inhalt und Umfang von TIAs werden durch die Empfehlungen 01/2020 sowie die Empfehlungen 02/2020[4] des Europäischen Datenschutzausschusses (EDSA) vorgegeben und dort detailliert erläutert. Im Wesentlichen müssen Datenexporteure eine rechtsvergleichende Untersuchung zwischen dem Recht des Drittlands und dem europäischen Datenschutzrecht anstellen – fundierte Kenntnisse sowohl des lokalen als auch des europäischen Rechts sind daher zwingend erforderlich.

Kern dieser Untersuchung ist die Frage, ob die Gesetze des Drittlands und die diesbezügliche Rechtspraxis den Datenimporteur daran hindern seine Pflichten aus dem jeweiligen Übermittlungsinstrument des Art. 46 DS-GVO zu erfüllen.[5] Dafür muss der Datenexporteur zunächst alle relevanten lokalen Gesetze sowie die relevante Gesetzespraxis identifizieren und verstehen, um sie dann mit den europäischen Rechtsstaatsgarantien zu vergleichen. Nur wenn er zum Ergebnis kommt, dass das Schutzniveau im Drittland dem europäischen Datenschutzniveau im Wesentlichen angemessen ist, darf er die Daten wie beabsichtigt übermitteln. Ist dies nicht der Fall, muss der Datenexporteur zusätzliche Maßnahmen implementieren. Hilft auch das nicht, darf die Übermittlung nicht stattfinden.[6]

[1] Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 in der Rechtssache C-311/18.

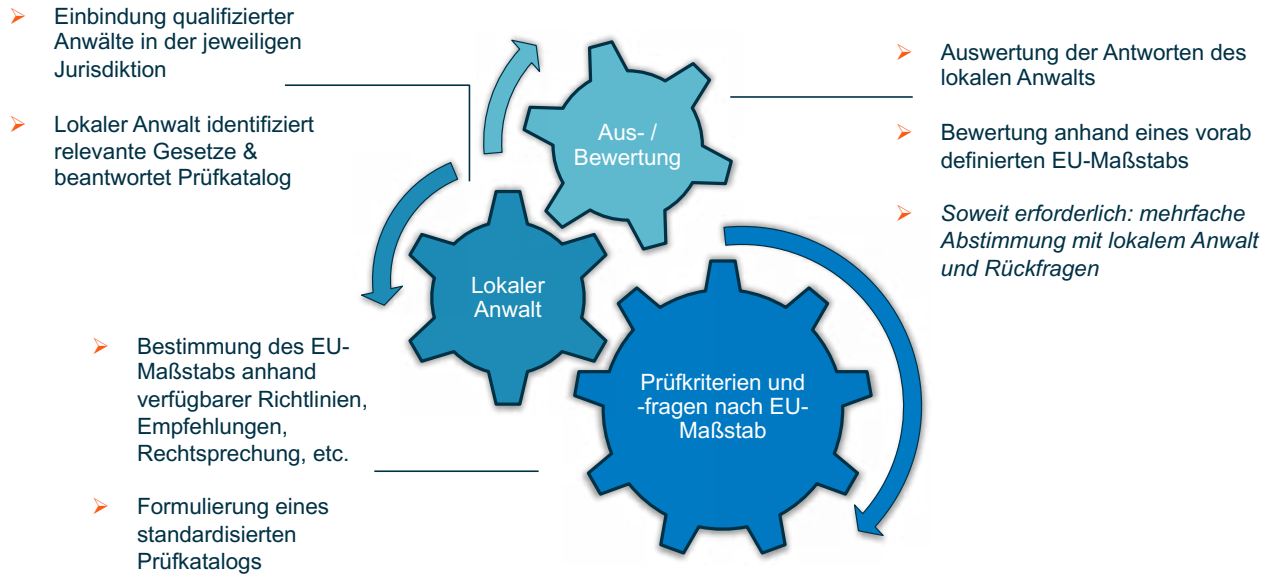
[2] Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten, Version 2.0, angenommen am 18. Juni 2021, („Empfehlungen 01/2020"), Rn. 28 ff.

[3] 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.

[4] Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen, angenommen am 10. November 2020, („Empfehlungen 02/2020").

[5] Empfehlungen 01/2020 Rn. 30.

[6] Empfehlungen 01/2020 Rn. 43.3.



Zusammenarbeit mit lokalen Anwälten bei Durchführung von TIAs (Illustration)

TIAs in der Praxis am Beispiel der VR China

Nachfolgend werden einige Ergebnisses eine in den Jahren 2022 und 2023 durchgeführten TIA für die VR China vorgestellt, die den Empfehlungen des EDSA folgen. Die Bewertung des lokalen Rechts erfolgte auf Grundlage von Informationen, die chinesische Rechtsanwälte zusammengestellt haben.

Ergebnisse des TIA

Das TIA bestätigt das Ergebnis einer vom EDSA in Auftrag gegebenen Studie aus dem Jahr 2021, die unter anderem auch das Datenschutzniveau der VR China untersucht hat.[7] Die im Rahmen des TIAs identifizierten chinesischen Sicherheitsgesetze („Anwendbare Gesetze") hindern lokale Datenimporteure daran ihre Pflichten aus den Standardvertragsklauseln zu erfüllen. Die Zugriffsbefugnisse chinesischer Behörden sind aus europäischer Sicht nicht erforderlich und angemessen. Der Umstand, dass China mit dem Personal Information Protection Law („PIPL") jüngst ein umfassendes Datenschutzgesetz eingeführt hat, ändert daran nichts, da das PIPL weniger vor behördlichen Zugriffen, als vor den Gefahren eines unregulierten Tech-Sektors schützen soll.[8]

Besonders deutlich zeigen dies die folgenden Punkte:

Behördliche Zugriffe unterliegen so gut wie keinen zeitlichen Beschränkungen. Den Anwendbaren Gesetzen fehlen Regelungen die z. B. mit § 100e Abs. 1 StPO vergleichbar sind. Ebenso fehlen Verfahrensregeln zum Umgang mit den von den Behörden erhobenen Daten.

Den Anwendbaren Gesetzen fehlen Regelungen zur Erforderlichkeit und Angemessenheit der auf Grundlage der chinesischen Sicherheitsgesetze erfolgenden Eingriffe. Vergleichbare Regelungen im deutschen Recht sind etwa die §§ 100a ff. StPO, die klar- und sicherstellen, dass Eingriffe auf das im Einzelfall erforderliche Maß beschränkt und angemessen sein müssen.

Die Anwendbaren Gesetze enthalten nur minimale Regelungen zur Information betroffener Personen oder des Datenexporteurs im Falle eines behördlichen Zugriffs auf personenbezogene Daten. Überwiegend gilt der – im Hinblick auf Art. 23 Abs. 2 lit. h) DS-GVO grundsätzlich akzeptable – Grundsatz, dass eine Information der Maßnahmenadressaten untersagt, bzw. nicht erforderlich ist, um den Zweck der Maßnahmen nicht zu gefährden. Sowohl betroffene Personen als auch der Datenexporteur können aber grundsätzlich eine höherinstanzliche bzw. verwaltungsrechtliche Überprüfung der Maßnahme bei Vorliegen eines begründeten Verdachts des behördlichen Datenzugriffs anstrengen.

Konsequenzen für Datenexporteure

Die im Rahmen des TIA identifizierten Defizite müssen Datenexporteure somit durch zusätzliche Maßnahmen (also Maßnahmen, die über die in den Standardvertragsklauseln enthaltenen Maßnahmen hinausgehen) ausgleichen.[9] Dies können technische, vertragliche oder organisatorische Maßnahmen sein. Allerdings ist nicht jede Art von Maßnahme gleich geeignet bestimmte Defizite auszugleichen.[10] Vielmehr müssen die gewählten Maßnahmen „genau die Rechtsschutzlücken

[7] Legal study on Government access to data in third countries, European Data Protection Board ("EDSA-Studie"), S. 55, abrufbar unter: https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.

[8] Johannes, ZD 2022, 90 (93 f.); zweifelnd auch EDSA-Studie, S. 22 f.

[9] Empfehlungen 01/2020 Rn. 50.

[10] Empfehlungen 01/2020 Rn. 47.

schließen, die der Datenexporteur [bei der Drittlandbewertung] festgestellt hat."[11] Angesichts dessen kann es auch einen Unterschied machen, ob Daten in ein Drittland nur übermittelt, dort (nur) gespeichert oder auch verarbeitet werden.

a. Identifikation und Bewertung möglicher risikoreduzierender Maßnahmen

Die im Rahmen des TIA identifizierten Defizite der Anwendbaren Gesetze sind nach der für dieses TIA entwickelten Bewertungslogik so gravierend, dass im Falle einer Verarbeitung durch einen in China ansässigen Datenimporteur nur technische Maßnahmen wie etwa eine möglichst umfassende Verschlüsselung der Daten (z. B. at rest, in memory) das Risiko reduzieren. Starke Verschlüsselungsmaßnahmen sind aber nicht immer auch praktikabel, etwa weil die meisten Dienstleister Zugriff auf die von ihnen verarbeiteten Daten im Klartext benötigen. Dieses Problem haben mittlerweile auch die Datenschutzbehörden selbst erkannt.[12]

Bei Ländern wie China, in denen sich die datenschutzrechtlichen Risiken aus grundlegenden strukturellen Defiziten (aus europäischer Grundrechtsperspektive) ergeben, also etwa der Klarheit von Eingriffsnormen, der Präzision der Eingriffsbefugnisse oder aus ihrer Erforderlichkeit und Angemessenheit, dürfte es schwerfallen mittels zusätzlicher vertraglicher Maßnahmen ein nach europäischen Maßstäben akzeptables Datenschutzniveau herzustellen. Anders gesagt: Zusätzliche Kontrollrechte für den Datenexporteur oder weitreichende Informationspflichten des Datenimporteurs machen defizitäre Sicherheitsgesetze eines Drittlands nicht besser. Einem in China ansässigen Datenimporteur zusätzliche vertragliche Pflichten aufzuerlegen führt in der Regel also nicht (vollständig) zum Ziel.

Dies gilt erst recht für organisatorische Maßnahmen. Diese dürften in den meisten Fällen den wenigsten Einfluss auf die Verbesserung des Schutzniveaus eines Drittlands haben, da es sich dabei um rein unternehmensinterne Maßnahmen handelt. [13] Am Ende bedarf es bei „Hoch-Risiko-Ländern" wie China daher wohl einer Umstellung des gesamten Verarbeitungsprozesses, z. B. von der Speicherung in China hin zur bloßen Übermittlung, damit sich ein aus datenschutzrechtlicher Sicht überhaupt noch akzeptables Risikoniveau ergibt.

b. Der risikobasierte Ansatz als Lösung?

Vor einer möglicherweise weitgreifenden Umstrukturierung von Datenverarbeitungsprozessen könnten Datenexporteure allerdings in Erwägung ziehen einen risikobasierten Ansatz zu verfolgen. Der risikobasierte Ansatz durchzieht die gesamte DS-GVO und soll die Pflichten des Verantwortlichen und des Auftragsverarbeiters ins Verhältnis zum Risiko der jeweils vorgenommenen Datenverarbeitung setzen.[14]

Ein Datenexporteur könnte z. B. argumentieren, dass angesichts der Rechtslage in einem Drittland zwar ein abstrakt hohes Risiko besteht, dass europäische Datenschutzstandards unterlaufen werden, das konkrete Risiko für eine Rechtsverletzung aufgrund der übermittelten Daten jedoch gering ist. Am Beispiel China: Wie wahrscheinlich ist es, dass chinesische Sicherheitsbehörden von ihren Zugriffsrechten Gebrauch machen und Rechte und Freiheiten von EU-Bürgern verletzen, wenn der dort ansässige Datenimporteur nur öffentlich zugängliche Geschäftskontaktdaten verarbeitet, welche die Behörden selbst anderweitig erlangen können?

Aus Sicht der europäischen Aufsichtsbehörden soll der risikobasierte Ansatz allerdings nicht für internationale Datentransfers gelten.[15] Wesentliches Argument hierfür ist unter anderem, dass sich in den Art. 44 ff. DS-GVO gerade kein Bezug auf ein Risiko finde und der EuGH in seiner „Schrems II"-Entscheidung sich nicht zum risikobasierten Ansatz geäußert habe.[16]

Dieser Meinung lassen sich gute Argumente entgegensetzen. So stellt etwa Erwägungsgrund 4 Satz 2 DS-GVO klar, dass „das Recht auf Schutz personenbezogener Daten kein uneingeschränktes Recht ist". Auch der EuGH hat bereits festgestellt, dass die in Art. 7, 8 GRCh niedergelegten Rechte keine absoluten Rechte sind. [17] Anführen ließe sich auch, dass der Risikogedanke in der DS-GVO auch dort gilt, wo sich der Begriff des Risikos nicht ausdrücklich im Gesetzestext findet – wie z. B. die unterschiedliche Behandlung personenbezogener und besonderer Kategorien personenbezogener Daten zeigt.[18]

[11] Empfehlungen 01/2020 Rn. 75.

[12] Siehe etwa die Feststellungen der AG DSK „Microsoft-Onlinedienste", Zusammenfassung, S. 7, am Beispiel Microsoft 365 oder BayLDA TB 2021, S. 46.

[13] Siehe die Beispiele in den Empfehlungen 01/2020 Rn. 128.

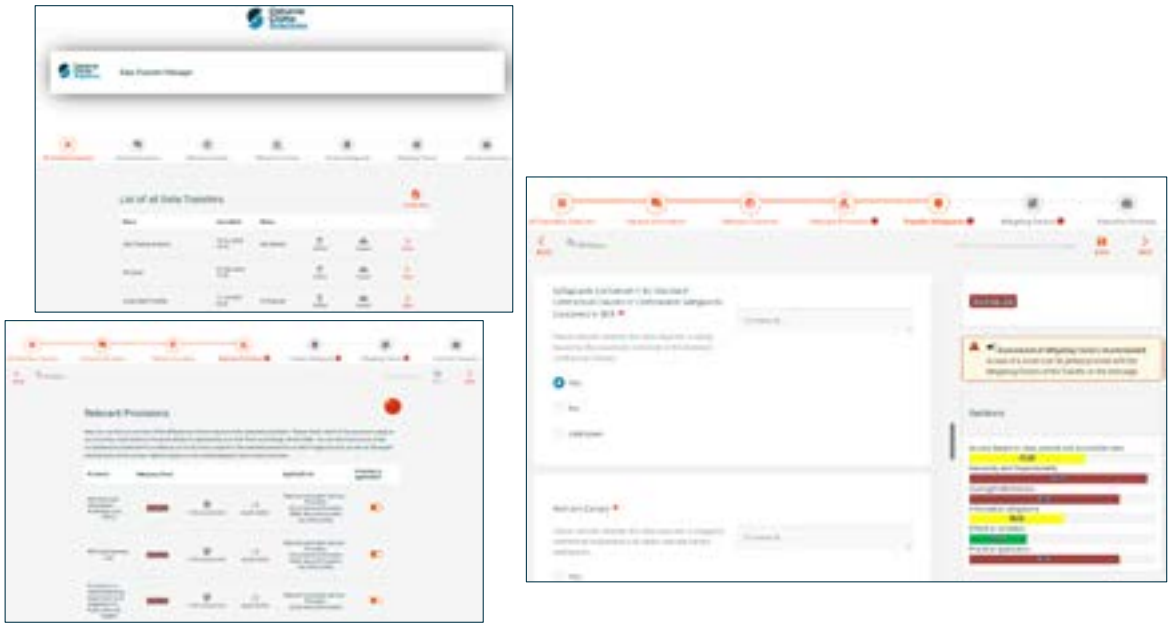
[14] Vgl. Amtsblatt EU C 159 v. 3. Mai 2016, 84; umfassend Schröder, ZD 2019, 503; siehe zB auch Taeger/Gabel/Lang, 4. Aufl. 2022, DSGVO Art. 24 Rn. 32; Ehmann/Selmayr/Heberlein, 2. Aufl. 2018, DSGVO Art. 24 Rn. 30.

[15] Siehe z.B. die Stellungnahme der CNIL zur Nutzung von Google Analytics, abrufbar unter: https://www.cnil.fr/en/qa-cnils-formal-notices-concerning-use-google-analytics, die Stellungnahme der dänischen Aufsichtsbehörde, abrufbar unter: https://www.datatilsynet.dk/english/google-analytics oder der Tätigkeitsbericht 2021 des Bayerischen Landesamts für Datenschutzaufsicht, S. 47.

[16] Siehe die Entscheidung der österreichischen Datenschutzbehörde vom 22. April 2022, S. 41, abrufbar unter: https://noyb.eu/de/oesterreichische-behoerde-lehnt-risikobasierten-ansatz-fuer-datenuebermittlungen-drittlaender-ab.

[17] EuGH ZUR 2011, 139 Rn. 48 (Schecke und Eifert / Land Hessen); ZD 2018, 23 Rn. 136 (EU-Kanada PNR-Abkommen); 2020, 31 Rn. 60 (Google LLC / CNIL).

[18] Mit weiteren Beispielen Jungkind/Koch ZD 2022, 656 (657).



Beispiel für eine Legal-Tech-Lösung zur Durchführung von TIAs

Ob der risikobasierte Ansatz auch im Rahmen von TIAs Anwendung finden kann, werden wohl die Gerichte entscheiden müssen. Bis dahin sollten risikoaverse Datenexporteure lieber der aufsichtsbehördlichen Meinung folgen und auf bestimmte Übermittlungen verzichten.

Durchführung von TIAs mit Legal-Tech-Lösungen?

Trotz der oben umrissenen hohen Anforderungen lassen sich TIAs in der Praxis sehr gut standardisieren und operationalisieren. Angesichts der recht konkret ausformulierten behördlichen Stellungnahmen und der darin beschriebenen Prüfungsstruktur können TIAs insbesondere auch sehr gut mit Legal-Tech-Lösungen bewältigt werden. Verantwortliche können hier entweder bereits auf die von Kanzleien angebotenen Lösungen zurückgreifen oder eigene Lösungen entwickeln. In der Praxis dürfte der Einkauf einer Legal-Tech-Lösung bei einer spezialisierten Kanzlei allerdings deutlich ressourcenschonender sein. Gerade internationale Kanzleien bieten hier Services aus einer Hand und stellen z. B. sicher, dass drittstaatliche Vorgaben regelmäßig auf ihre Aktualität geprüft werden und ausreichend kompetente lokale Anwälte im erforderlichen Umfang in TIAs eingebunden werden.

Über den Autor

Dr. Florian Eisenmenger, CIPP/E, CIPM, FIP
ist Fachanwalt für IT-Recht und Datenschutzexperte bei der internationalen Wirtschaftskanzlei Osborne Clarke. Er berät Unternehmen zu allen Fragen des Datenschutzrechts und hat maßgeblich an der Entwicklung einer Legal-Tech-Lösung für die Durchführung von TIAs mitgewirkt.

FAZIT

Die Übermittlung personenbezogener Daten nach China ist angesichts der nach europäischem Grundrechtsmaßstab bestehenden Defizite chinesischer Sicherheitsgesetze grundsätzlich nur sehr eingeschränkt zulässig. Mit Hilfe des risikobasierten Ansatzes tun sich aber ggf. etwas weitere Spielräume für Datenexporteure auf. Da europäische Aufsichtsbehörden diesen Ansatz in diesem Kontext jedoch nicht für zulässig halten, sollten Datenexporteure unter Umständen bereit sein ihre Rechtsauffassung auch streitig gegenüber einer zuständigen Behörde zu vertreten. Allerdings wurde bislang noch nicht bekannt, dass TIAs substanziiert von Aufsichtsbehörden geprüft wurden oder Behörden gar Sanktionen wegen deren fehlerhafter Durchführung verhängt hätten.

Was nicht ist, kann aber natürlich noch werden und TIAs dürften alsbald nicht an Relevanz verlieren. Um es mit einem Zitat aus der Popkultur zu sagen: „Es gibt viel zu viel Ausland auf der Welt" – bislang aber gerade einmal 15 Angemessenheitsentscheidungen. Auf die europäischen Aufsichtsbehörden dürfte also viel Arbeit zukommen, wenn bezüglich der Vorgaben der Art. 44 ff. DS-GVO kein Vollzugsdefizit herrschen soll.

CARMEN WEGGE

BESCHÄFTIGTENDATEN-SCHUTZGESETZ

Modernes Arbeitnehmerschutzgesetz in der Digitalisierung.

Demokratie endet nicht am Werkstor, das sagen wir in der SPD und in den Gewerkschaften immer gerne. Aber wir müssen auch sagen können: Datenschutz endet nicht am Werkstor.

Im Datenschutz geht es eben nicht nur um den Schutz von personenbezogenen Daten von Kund*innen, Kooperationspartner*innen oder Lieferant*innen, sondern auch und speziell um den Schutz der personenbezogenen Daten von Mitarbeiter*innen. Neben der DSGVO haben wir als Rechtsgrundlage die nationale Vorschrift des § 26 Bundesdatenschutzgesetz (BDSG). § 26 BDSG hat acht Absätze, die die nationale Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Beschäftigungsverhältnis darstellen. In acht Absätzen – und das schreibe ich als Juristin – kann viel stecken. Aber für das weite Feld des Beschäftigtendatenschutz reichen acht Absätze nicht aus.

Ich finde es wichtig, dass Beschäftigte ganz klar wissen, was ihre Rechte sind. Dass ich nicht erst Gerichtsurteile suchen muss, die zu meinem Fall passen, sondern am besten in ein Gesetz schauen kann, um die Antwort zu finden. Oder um zumindest eine eine Ahnung davon zu bekommen, ob es in meinem Fall mit „rechten Dingen“ zugeht oder nicht. Deshalb haben wir im Koalitionsvertrag von SPD, Bündnis 90/Die Grünen und FDP unseren Anspruch formuliert eigenständige Regeln für den Beschäftigtendatenschutz zu schaffen.

Wir wollen Rechtsklarheit für die Beschäftigten und Arbeitgeber*innen. Wir wollen den Schutz der Persönlichkeitsrechte für alle Beschäftigten gewährleisten, die ihn benötigen. Vor allem die immer größer werdenden technischen Möglichkeiten des Leistungstrackings und der automatisierten Verarbeitung von verschiedenen Datenarten erfordern es unser Recht fürs Zeitalter der Digitalisierung fit zu machen. Wenn wir es gut machen, und das ist das Ziel, schaffen wir damit eine neue Grundlage für den Schutz der Beschäftigten in der Transformation.

Im Frühjahr 2023 haben das Arbeits- und das Innenministerium gemeinsame Eckpunkte für das Beschäftigtendatenschutzgesetz erarbeitet. Diese wurden mit verschiedenen Stakeholdergruppen auf Herz und Nieren geprüft. Die Rückmeldung von Betriebs- und Personalräten, Arbeitgeber*innen, Zivilgesellschaft und Rechtsexpert*innen fließt nun in die Erarbeitung des Gesetzentwurfs ein. Ich rechne noch in diesem Jahr mit dem Start des Gesetzgebungsprozesses. Nach der Verabschiedung im Bundeskabinett werden wir

Abgeordnete uns dann vermutlich im Frühjahr 2024 im Bundestag intensiv mit dem Gesetz auseinandersetzen und es beschließen.

Die Fragen, die wir lösen wollen, sind nicht einfach, aber das soll uns nicht entmutigen. Wir wollen zum Beispiel Regelungen für typische Datenverarbeitungsvorgänge im Beschäftigungskontext vorsehen, die auf Künstlicher Intelligenz bzw. Algorithmen basieren. Dabei wollen wir insbesondere die Transparenz für Beschäftigte stärken.

Ich bin davon überzeugt: Den Fortschritt, den unser Land so dringend braucht, die Transformation in eine digitale Industriegesellschaft, das werden wir nur schaffen mit Zuversicht und Vertrauen. Vertrauen in die Digitalisierung bekommen wir aber nur hin, wenn technische Systeme für die Menschen keine Blackboxes sind und wenn sie verstehen, was mit ihren Daten passiert. Wenn sie zu jedem Zeitpunkt einwilligen oder widersprechen können. Wenn sie passgenau einstellen können, was sie mit wem teilen wollen. Und wenn sie und ihre Leistungen nicht permanent überwacht werden.

Deshalb hoffe ich auch, dass auch die bisherigen Zauderer verstehen, dass Beschäftigtendatenschutz kein Bürokratiemonster ist. Wenn wir es gut machen, wird das ein neues Grundgesetz für Beschäftigung in der Digitalisierung. Eine Grundlage, auf dem das Vertrauen wachsen kann und die Beschäftigten den Wohlstand unseres Landes weiter voranbringen.

Ich sehe das Beschäftigtendatenschutzgesetz daher auch nicht unter dem Label Datenschutz, sondern tatsächlich als ein modernes Arbeitnehmerschutzgesetz für die nächsten 100 Jahre. Packen wir es an!

Über die Autorin

Carmen Wegge
ist seit 2021 Mitglied im Innen- und im Rechtsausschuss des Deutschen Bundestages und in der SPD-Fraktion für Gesetzgebung rund um den Datenschutz zuständig.

HARALD TRETTOW

AUFTRAGSVERARBEITUNG NACH ART. 28 ABS. 3 LIT. G DS-GVO

Die Löschung oder Rückgabe von Daten und das Löschen von Kopien bei Verarbeitungsende – eine Exit-Strategie.

Das Ziel des Artikel 28 Abs. 3 lit. g DSGVO (Datenschutz-Grundverordnung 2016/679) ist darauf ausgerichtet, dass nach Abschluss der Verarbeitungsleistung des Auftragsverarbeiters (Art. 4 Nr. 8 DSGVO) keine personenbezogenen Daten des Verantwortlichen (Art. 4 Nr. 7 DSGVO) länger bei dem Auftragsverarbeiter vorhanden sind und/oder ein Zugriff auf personenbezogene Daten des Verantwortlichen durch den Auftragsverarbeiter nicht mehr möglich ist.

Rechtliche Vorgaben aus der DSGVO

Nach dem Wortlaut des Art. 28 Abs. 3 lit. g DSGVO hat der Auftragsverarbeiter nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben und vorhandene Kopien zu löschen[1], sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Der Verantwortliche sollte daher das Verfahren zur Rückgabe überlassener Datenträger oder die sichere Löschung der gespeicherten Daten für den Zeitpunkt der Beendigung der Auftragsverarbeitung schon bei Vertragsbeginn durch Weisung festlegen. Auch die Regelung, dass der Verantwortliche während der Laufzeit des Vertrages oder bei dessen Beendigung die bei Vertragsschluss getroffene Wahl durch Weisung noch abändern kann sollte vertraglich verankert werden.[2]

Weiterhin sollte ersichtlich und eindeutig dokumentiert sein, in welchem Zeitrahmen oder auch zu welchem genauen Zeitpunkt eine Löschung oder Rückgabe zu erfolgen hat. Zudem sollte sich der Verantwortliche aufgrund seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nach einer Löschung der Daten durch den Auftragsverarbeiter bestätigen lassen, dass die Löschung innerhalb des vereinbarten Zeitrahmens oder zu dem vereinbarten Zeitpunkt und in der vereinbarten Form nachweislich erfolgt ist.[3] Dies umfasst auch die Löschung vorhandener Kopien, welche sich oftmals – insbesondere bei Cloud-Diensten – nicht nur an einer zentralen Stelle oder an einem zentralen Standort befinden können, sondern möglicherweise gesplittet an unterschiedlichen geografischen Standorten oder in sogenannten „Cold Storages“[4] gespeichert sind.

Da das Wahlrecht – Löschen oder Zurückgeben – nach Art. 28 Abs 3 lit. g DSGVO ausschließlich dem Verantwortlichen obliegt, muss dieser spätestens bei Vertragsende eine entsprechende Weisung erteilen.

Risiken bei und nach Abschluss der Erbringung der Verarbeitungsleistung

Es gehört zur allgemeinen Risikobewertung eines Unternehmens sich schon vor einer Auslagerung von personenbezogenen Daten Gedanken darüber zu machen und zu bewerten, welche (datenschutz-)rechtlichen, wirtschaftlichen und technischen Risiken nicht nur während der Auslagerung der Verarbeitung auftreten können, sondern auch über Risiken bei Verarbeitungsende beziehungsweise Vertragsbeendigung mit einem externen Dienstleister. Auch in Hinsicht auf eine fristlose Kündigung sollten Regelungen getroffen werden, welche es dem Verantwortlichen ermöglichen seinen Geschäftsbetrieb ohne Einschränkungen fortführen zu können. Gerade bei einer fristlosen Kündigung aus wichtigem Grund sind ausschweifende Auseinandersetzungen nicht unüblich.

Es ist daher dringend dazu geraten ein Zurückbehaltungsrecht i. S. V. § 273 BGB durch den Auftragsverarbeiter bei Vertragsabschluss auszuschließen.

Dies ist auch die Ansicht von einigen deutschen Aufsichtsbehörden (unter anderem vertritt der Hessische Beauftragte

[1] Amtsblatt der Europäischen Union L 127, S.4, 61. Jahrgang, 23. Mai 2018

[2] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, 07 July 2021, 140

[3] Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, 07 July 2021, 141

[4] „Cold Storage“ wird im IT-Bereich so verstanden, dass nicht aktive oder selten genutzte Daten auf einem Medium gespeichert werden, auf welchem der Zugriff und die Verarbeitungszeiten zeitlich erhöht sind, im Vergleich zu den Daten und Datenspeicher, auf welche ein schneller und sehr häufiger Zugriff notwendig ist oder gefordert wird.

für Datenschutz und Informationsfreiheit diese Position), welche eine entsprechende Klausel in ihren Formulierungshilfen[5] für einen Auftragsverarbeitungsvertrag aufgenommen haben, so auch das Bayerische Landesamt für Datenschutz in seiner Orientierungshilfe zur Auftragsverarbeitung[6].

Art und Weise einer Rückgabe

Innerhalb der vertraglichen Bindung und zur Klarstellung sollte eine Klausel vorliegen, auf welche Art und Weise die Rückgabe der Daten zu erfolgen hat. Zu differenzieren wäre zwischen der Rückgabe von physischen Datenträgern (zum Beispiel Papierakten), physischen Datenträger mit Speicherfunktion oder der Rückgabe durch Übermittlung/Übertragung digitaler Daten.

Digitale Datenrückgabe

Aufgrund der heutzutage überwiegenden digitalen Speicherung von Daten auf Datenträgern wie USB-Sticks, (Server-) Festplatten oder in der Cloud sollte eine Rückgabe oder Rückübermittlung bei einem gängigen und maschinenlesbaren Datenformat problemlos und nur mit sehr geringem Aufwand möglich und daher auch nicht kostenintensiv bis nicht kostenpflichtig sein.

Ein weiterer wichtiger Aspekt des Verantwortlichen sollte immer die störungsfreie und problemlose Verwendbarkeit der zurückerhaltenen Daten sein. Daher ist es zu empfehlen eine frühzeitige und gestaffelte Rückgabe von Datenbeständen in einem gängigen und kompatiblen Datenformat zu vereinbaren, so dass nach erfolgreichem Testen der Migrationsfähigkeit in die eigene IT-Infrastruktur oder in die eines anderen (Cloud-)Dienstes technische Probleme bei der endgültigen Rückgabe bei Vertragsende stark reduziert sind oder sogar vollständig vermieden werden können. Falls allerdings eine Unterstützungsleistung des Anbieters zur Migration in ein proprietäres Datei- oder Datenbankformat eines anderen (Cloud-)Dienstleisters oder Softwareanbieters erforderlich wird, wäre es sicherlich denkbar eine transparente und angemessene Kostenregelung in Betracht zu ziehen und vorzugsweise in einem gesonderten Vertrag – etwa im Hauptvertrag – zu vereinbaren oder mit einzufügen.

Rückgabe oder Löschen (zum Beispiel durch Vernichten) von physischen Datenträgern

Wie eine Rückgabe von Datenträgern oder physikalischen Datenträger mit Speicherfunktion sinnvoll und datenschutzgerecht erfolgen kann, hängt von den Gesamtumständen der Verarbeitungstätigkeit ab, unter anderem davon, wo die Verarbeitung tatsächlich geografisch erfolgt und mit welchem Aufwand ein Transport der Datenträger datenschutzkonform erfolgen kann. Der Aufwand ergibt sich unter anderem aus der Zusammenführung und Betrachtung aller erforderlichen technischen und organisatorischen Maßnahmen und anfallenden Kosten, insbesondere aus Transportkosten, personellem Aufwand, Dauer und Wege des Transportes, den zur Verfügung stehenden Transportmitteln und den sich aus diesen Faktoren ergebenden Risiken.

[5] https://datenschutz.hessen.de/infothek/hinweise-und-muster-zur-ds-gvo, Stand 14.01.2022

[6] Orientierungshilfe Auftragsverarbeitung, Der Bayerische Landesbeauftragte für den Datenschutz, Version 2.0, 1. April 2019, S. 20

Um die Risiken eines manuellen Transportes zu vermeiden, besteht aber auch die Möglichkeit das Löschen von Daten auf Datenträgern dem Auftragsverarbeiter aufzuerlegen.

Falls der Verantwortliche dem Auftragsverarbeiter Datenträger bereitgestellt hat, wird im Regelfall die Form des Löschens durch Vernichten des Datenträgers angewendet und oft mit Inanspruchnahme eines weiteren, spezialisierten Dienstleisters umgesetzt. Hier liegt es also im Ermessen des Verantwortlichen, ob er sich Datenträger sicher und datenschutzkonform zurückgeben lässt oder ob der Verantwortliche den Auftragsverarbeiter mit der Löschung der Daten durch Vernichtung (als Unterform einer Löschung) der Datenträger beauftragt.

Diese zusätzliche Beauftragung eines oft spezialisierten Dienstleisters kann mit weiteren Kosten für den Verantwortlichen verbunden sein, falls diese Zusatzleistung nicht schon in dem Hauptvertrag mit eingepreist wurde. Der Aufwand und der Umfang einer Datenträgervernichtung hängt zwangsweise von dem zu erwartenden Datenvolumen und der sich daraus resultierenden Anzahl der notwendigen Datenträger ab, diese sollten sich aber im Groben abschätzen lassen oder im Regelfall genau zu ermitteln sein.

Aufgrund einer gesamtheitlichen Bewertung insbesondere mit Blick auf die Datensicherheit sowie auf Aufwand und Kosten, sollte der Verantwortliche gewissenhaft entscheiden, welches Verfahren er zur Rückgabe von Daten auf Datenträgern wählt, vor allem unter Berücksichtigung datenschutzrechtlicher Aspekte, wie der Gewährleistung, dass beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten sichergestellt ist (Transportkontrolle) und dass ein Transport unter Berücksichtigung der gesetzlichen Vorgaben aus Artikel 32 DSGVO erfolgt.

Bei Clouddiensten wie SaaS und PaaS müssen andere Löschmethoden angewendet werden.

Löschen durch Überschreiben und Anonymisieren von Daten

Weitere sichere und anerkannte Methoden des Löschens sind das Anonymisieren von Daten und das mehrfache Überschreiben von Datenträgern, das sogenannte „Wiping“, welches ein Auftragsverarbeiter zum Löschen der personenbezogenen Daten des Verantwortlichen durchführen kann.

Überschreiben von Daten

Maßgebliche Kriterien einer sicheren und geeigneten Löschung sind die Wirksamkeit der angewendeten Algorithmen, daher sollte der Anbieter dem Verantwortlichen die Anwendung anerkannter nationaler oder internationale Standard-Algorithmen bestätigen und welche Zertifizierungen (zum Beispiel EAL3+ der Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) und Empfehlungen unabhängiger dritter Stellen im Bereich Datenlöschung vorliegen.

Bei der logischen Löschung von Daten ist es dringend empfohlen die zur Verfügung stehenden Löschmethoden und Art und Umfang von Löschprotokollen des Anbieters als weiteres Kriterium bei der Auswahl eines Dienstleisters mit einfließen zu lassen.

Protokollierung von Löschungen

Die meiste derzeit auf dem Markt befindliche Softwares zum sicheren Löschen von Daten (auch SaaS) bietet die Möglichkei ein Löschprotokoll in Form von unterschiedlichen exportierbaren Berichtsformate wie XML, HTML, XLS und PDF zu erstellen. Daher sollte der Verantwortliche sich jedenfalls diese detaillierten Berichte nicht nur zur Kontrolle einer Löschtätigkeit des Auftragsverarbeiters regelmäßig während der Vertragslaufzeit, sondern insbesondere nach der endgültigen Löschung von personenbezogen Daten bei Vertragsende beziehungsweise Verarbeitungsende zur Verfügung stellen lassen. Dieser anschließende und abschließende Löschnachweis dient daher als Zeitpunkt der tatsächlichen Beendigung der Auftragsverarbeitung.

Anonymisieren von Daten

In dem verbindlichen Teil der DSGVO wird der Begriff Anonymisierung nicht angewendet. In Erwägungsgrund 26 wird nur dazu Stellung genommen, dass die DSGVO nicht anwendbar ist bei anonymisierten Daten, also auf solche, welche sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert oder so verändert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.

Daher stellt die Entfernung des Personenbezugs von personenbezogenen Daten grundsätzlich ein mögliches Mittel zur Löschung i.S.v. Art. 4 Z. 2 i.V. m. Art. 17 Abs. 1 DSGVO dar. Es muss jedoch sichergestellt werden, dass weder ein Dritter noch der Verantwortliche selbst ohne unverhältnismäßigen Aufwand einen Personenbezug wiederherstellen kann. Hierzu ist aber immer ein Augenmerk auf den Stand der Technik zu legen.

Das Anonymisieren von Daten stellt nach der Auffassung der österreichischen Datenschutzbehörde eine Form des

Löschens dar[7] und somit kann der Verantwortliche der Datenverarbeitung nach seiner Wahl und seinem Ermessen auch den Auftragsverarbeiter dazu anweisen die von der Auftragsverarbeitung betroffenen personenbezogenen Daten mit dieser Methode zu löschen.

Cloud-Dienste

Der Verantwortliche muss die besonderen Risiken des Cloud-Computing umfassend ermitteln und bewerten, die sich aus der angedachten Nutzung eines externen Cloud-Dienstes ergeben können.

Bei den zu ermittelnden Risiken sollte auf jeden Fall die Art und Weise einer Datenrückgabe und das Löschen personenbezogener Daten beim Auftragsverarbeiter berücksichtigt werden. Hier ist der Fokus auf vorhandene Export- oder Migrationsmöglichkeiten und Löschverfahren während der Auftragsverarbeitung und auch bei Beendigung des Vertrages bzw. der Verarbeitungstätigkeit zu richten.

Um nicht bei Vertragsende von technischen Hemmnissen (etwa von technischen Beschränkungen oder Voraussetzungen) oder zusätzlichen Kosten überrascht zu werden, sollte der Verantwortliche vor Vertragsschluss ein Blick auf das dazu vom Cloudanbieter verwendete Datenformat und Betriebssystem werfen und welche entsprechenden Regelungen – aber auch Möglichkeiten – der Cloud-Dienstleister in seinem Angebot, Vertrag, AGB oder vergleichbaren Dokumenten dazu vorsieht.

Falls der geplante Cloudanbieter ein eigenes, nicht marktübliches und proprietäres Datenformat oder Betriebssystem anwendet, bestehen die nicht zu unterschätzenden Risiken für den Verantwortlichen einer fehlenden oder nicht ausreichenden Interoperabilität des Datenformates oder einer Inkompatibilität des Betriebssystems zu seiner eignen IT-Struktur oder zu denen weiterer Anbieter von Cloud-Dienstleistungen bei einer Datenrückgabe bzw. Datenweitergabe.

Eine vertraglich vereinbarte und detaillierte Exit-Strategie kann dem Cloudanwender dazu dienlich sein eine detaillierte Kosten- und Investitionsplanung zu erstellen und sich eine gewisse Unabhängigkeit in Hinblick der immens steigenden Anzahl von Cloud-Softwarelösungen verschiedener Anbieter zu bewahren oder zu schaffen. Auch in Hinblick auf eine mögliche Insolvenz oder Einstellung eines Cloud-Dienstes ist eine geregelte Exit-Strategie unverzichtbar.

Dies spiegelt das Ergebnis einer Befragung von 555 Unternehmen in Deutschland durch die Bitkom Research GmbH im Auftrag des Beratungsunternehmens KPMG wider. In der Veröffentlichung des „Cloud-Monitor 2020“ im Jahr 2020 befand sich eine vertraglich regelbare Exit-Strategie unter den TOP 5 Kriterien bei der Auswahl für Cloud Dienstleistungen und deren Anbieter.[8]

Daher sollten alle Informationen über vertragliche, technische und organisatorische Gegebenheiten, der von den Cloud-Dienstleistern angebotenen Cloud-Dienstleistungen einschließlich detaillierter und nachvollziehbarer Sicherheitskonzepte bezüglich der Rückgabe und Löschung von personenbezogenen Daten dem Verantwortlichen im Vorfeld vorliegen, so dass der Verantwortliche diese datenschutzrechtlich bedeutsamen Entscheidungskriterien bei der sorgfältigen Auswahl zwischen den Anbietern zur Verfügung hat und sich nicht nur rein aus wirtschaftlichen Gründen möglicherweise für einen finanziell günstigeren Anbieter mit höheren (Sicherheits-)Risiken entscheidet.

FAZIT

Zur Erhöhung des Sicherheitsniveaus und der Erfüllung der Rechenschaftspflicht gemäß Artikel 5 Abs. 2 DSGVO sollte der Verantwortliche eine detaillierte und transparente Regelung zur Löschung und Rückgabe der personenbezogenen Daten bei Beendigung der ausgelagerten Verarbeitungstätigkeit schriftlich oder in einem elektronischen Format schon bei Vertragsabschluss vereinbaren.

Diese Regelung verhindert nicht nur mögliche Unklarheiten, Beeinträchtigungen des Geschäfts- oder Produktionsbetrieb des Verantwortlichen und Auseinandersetzungen zwischen den Parteien bei oder nach Vertragsende, sondern eine regelbare Exit-Strategie stellt sogar ein gewichtiges Kriterium schon bei der Auswahl eines externen Dienstleisters dar und kann auch als Nachweis als Teil einer erfolgten Risikoanalyse des Verantwortlichen dienen.

Über den Autor

Harald Trettow
ist interner und externer Datenschutzbeauftragter.
Er ist außerdem langjähriges Mitglied im
BvD und in der GDD.

[7] Österreichische Datenschutzbehörde, DSB-D123.270/0009-DSB/2018 vom 5.12.2018

[8] Cloud-Monitor 2020, Studie von Bitkom Research GmbH im Auftrag von KPMG

STANDARD-DATENSCHUTZ-MODELL 3.0

Martin Rost

Die deutschen Datenschutzaufsichtsbehörden (DSK) haben Ende 2022 das Standard-Datenschutzmodell (SDM) in der Version V3 als Prüf- und Beratungsstandard zur Umsetzung der Anforderungen der DSGVO bestätigt.

Die Aufgabe des SDM

Die Aufgabe des SDM besteht darin die normativen Anforderungen an eine Verarbeitung mit Personenbezug in eine methodisch kontrollierte Beziehung zu wirksamen Schutzmaßnahmen zu setzen. Die „Grundsätze" des Art. 5 Abs. 1 DSGVO werden dafür als (Gewährleistungs-)„Ziele" reformuliert und mit konkreten Standard-Schutzmaßnahmen hinterlegt. Ziele erlauben eine interdisziplinäre Zusammenarbeit von Jurist*innen, Techniker*innen, IT-Security-Expert*innen, Betriebswirt*innen und Verantwortlichen bei der Gestaltung von Verarbeitungen; der Ausweis von Standardmaßnahmen zur Risikominimierung erlaubt die Kalkulation von Kosten.

Das SDM hat in vielen Unternehmen Einzug gehalten, der Grund ist klar: Das SDM macht eine standardisierte Umsetzung von Anforderungen der DSGVO betriebswirtschaftlich realistisch kalkulierbar. Einige Firmen haben aber auch ihre Kritik hinsichtlich der Anwendbarkeit im praktischen Betriebsalltag geäußert, die im SDM 3.0 berücksichtigt wurde.

SDM-V3 mit neuem Fokus

Was ist neu? Das SDM-V3 stellt, klarer als in den Vorversionen, die Verarbeitung personenbezogener Daten in den Vordergrund (s. Art. 1 DSGVO) und macht diese anhand von drei Dimensionen analysierbar und gestaltbar. Welche Dimensionen sind das?

Zum einen wird im SDM-V3 die Liste der 14 Verarbeitungsvorgänge (s. Art. 4 Nr. 2 DSGVO) auf 9 Vorgänge oder 4 Phasen verkürzt. Für eine als wenig riskant beurteilte Verarbeitung kann es ausreichen, nur die Erhebung, die Bereithaltung, die Nutzung und die Beseitigung personenbezogener Daten zu unterscheiden und hinsichtlich der Risiken für Betroffene zu bearbeiten. Dies ermöglicht eine phasenspezifische Bestimmung von Rechtsgrundlagen und Schutzmaßnahmen. So sind bspw. Schutzmaßnahmen zur Umsetzung der Zweckbestimmung (durch Trennung von Systemen) oder Vertraulichkeit (durch Verschlüsseln von Daten und Kommunikationsverbindungen) beim Nutzen von Daten andere als beim Erheben, Bereitstellen oder Löschen von Daten.

Zum zweiten gilt es, bei jeder Verarbeitung drei Ebenen zu unterscheiden: Die Ebene 1 entspricht einem „Fachverfahren" bzw. „Geschäftsprozess" als einem abstrakten, funktionalen Ablauf; hier werden die Legitimität des Zwecks und die Logik der Abläufe abstrakt bestimmt. Die Ebene 2 fokussiert die konkrete Implementation dieser Abläufe mit Hilfe von Sachbearbeitung und IT-Fachapplikation(en). Die Ebene 3 umfasst die IT-Infrastruktur, mit zentralen IT-Funktionen für die Ebene 2, die in Form von „Diensten" zumeist von Rechenzentren als Auftragsverarbeitern bereitgestellt werden.

Fügt man zu den „Phasen" und „Ebenen" die bekannten „Gewährleistungsziele" des SDM hinzu, hat man drei Dimensionen zusammengestellt und nimmt damit den „SDM-

Abbildung: Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz).

Würfel“ in den Blick, die Hauptinnovation des SDM-V3 (s. SDM-V3, S. 46). Die sieben Gewährleistungsziele fungieren als Bezeichner für spezifische Risiken die in den Phasen und Ebenen erzeugt werden und entsprechend zu analysieren, zu beurteilen und zum Nutzen der Personen zu verringern sind. Hiernach besteht bspw. ein Risiko darin, dass durch die Verarbeitung mit Hilfe einer Fachapplikation in der Phase der Datenerhebung keine Prüfbarkeit (Transparenz) gegeben ist, wenn diese Aktivität der Erhebung nicht spezifiziert, dokumentiert und protokolliert wird.

Jeder Subwürfel des SDM-Würfels steht für ein aus der DSGVO abgeleitetes Risiko, das bei einer Verarbeitung mit Hilfe von Schutzmaßnahmen zu bearbeiten und auf ein rechtlich verantwortbares Maß zu verringern ist. Der SDM-Würfel stellt auf diese Weise ein Gesamtbild sämtlicher zu bearbeitenden Datenschutzrisiken bei einer Verarbeitungstätigkeit einer Organisation dar.

SDM im Betriebsalltag

Der 2021 in einem Fachaufsatz erstmals veröffentlichte SDM-Würfel wurde von einigen Programmherstellern inzwischen aufgegriffen. Die Unterarbeitsgruppe SDM des AK-Technik (UAGSDM) hatte Anfang 2023 eine Sichtung von SDM-Tools durchgeführt. Dabei zeichnet sich eine neue Entwicklung ab: Nachdem das Abarbeiten der Maßnahmenlisten des SDM zumeist mit Hilfe von Tabellenkalkulationen dokumentiert wurde, erlaubt der Rückgriff auf den SDM-Würfel die Entwicklung von SDM-Tools als Wizzards.

Diese Tools führen die Nutzer*innen systematisch durch die Modellierung von Verarbeitungen, durch Prüfprozesse oder das dauerhafte Controlling von Schutzmaßnahmen im Rahmen eines Datenschutzmanagementsystems. Wann diese Tools aus den großen Sozietäten und Beratungshäusern heraus reif für den Markt entwickelt sind ist noch nicht abzuschätzen.

Tools sind aber nicht immer die angemessenste Lösung. Bei Verarbeitungen mit einem relativ kleinen Umfang sollten sich Verantwortliche an ihre Interessensvertretungen (bspw. Handwerkskammern, IHK, BDI, Ärzte- und Apothekerverbände, Rechtsanwalts- oder Notariatskammern) wenden und bspw. Datenschutz-Folgenabschätzungen für die typischen Verarbeitungen ihrer Branche oder ihres Geschäftszweigs auf der Grundlage des SDM erarbeiten lassen, so dass vor Ort nur noch ein schlankes Customizing der Verarbeitungen notwendig wird.

FAZIT

Der neue SDM-Würfel des SDM-V3 stellt vollständig sämtliche Anforderungen der DSGVO an eine personenbezogene Verarbeitung vor Augen und unterstützt ggfs. eine gut begründbare Reduktion der Komplexität einer personenbezogenen Verarbeitung. Das spart Aufwand im Rahmen von Datenschutzprüfungen, Datenschutz-Folgenabschätzungen und beim Datenschutzmanagement.

Über den Autor

Martin Rost
ist Mitarbeiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) und u.a. Leiter der Arbeitsgruppe zur Entwicklung des „Standard-Datenschutzmodells“ (SDM).

▶ mail@datenschutzzentrum.de

THOMAS KAHL, TERESA KIRSCHNER

NIS-2 UND DER „NEUE“ RECHTSRAHMEN FÜR DIE IT-SICHERHEIT IN EUROPA

Was kommt auf Unternehmen zu?

Der Schutz vor Cyberattacken gehört zu den Kernaufgaben der Unternehmensführung. Aber die Praxis sieht manchmal anders aus. Verstärken große Unternehmen zusehends ihre Bemühungen im Bereich der IT-Sicherheit, finden sich immer noch viele Unternehmen, bei denen die IT-Sicherheit noch nicht „Chefsache“ geworden ist. Um den europäischen Binnenmarkt vor der Bedrohungslandschaft zu schützen und insbesondere Betreiber kritischer Dienstleistungen und Produkte zukünftig widerstandsfähiger gegen Cyberangriffe zu machen, verschärft der EU-Gesetzgeber sukzessive die Anforderungen an die IT-Sicherheit auch für Unternehmen, die bislang von entsprechenden Regelungen (noch) nicht betroffen sind. Kernstück der Bemühungen um europaweit einheitliche und höhere IT-Sicherheitsstandards in besonderen Wirtschaftsbereich ist die Network and Information Security Directive, kurz NIS-2, die bis zum Oktober 2024 in nationales Recht umgesetzt sein muss. Der folgende Beitrag widmet sich den mit der NIS-2 auf Unternehmen zukommende Änderungen und ordnet das Regelwerk in den zukünftigen Rechtsrahmen zur IT-Sicherheit in der EU ein.

1. NIS-2 – Worum geht’s?

Die Richtlinie (EU) 2022/2555[1] „The Network and Information Security Directive“ (NIS 2) ersetzt die im Jahr 2016 in Kraft getretene NIS-RL. Mit dieser wurden erstmals umfassende Regelungen für Cybersicherheit im Bereich besonders kritischer Infrastrukturen auf europäischer Ebene verabschiedet.

In Deutschland wurden die Vorgaben im BSIG umgesetzt. Am 27.12.2022 wurde die NIS-2 im EU-Amtsblatt veröffentlicht und ist zum 16.01.2023 in Kraft getreten. Durch die Richtlinie und deren Umsetzung in den Nationalstaaten soll ein erhöhtes Niveau der Cyberresilienz in der EU geschaffen und der europäische Binnenmarkt besser vor Cyberangriffen geschützt werden. Die Mitgliedstaaten haben bis Oktober 2024 Zeit zur Umsetzung der Regelungen in nationales Recht. Seit Juli 2023 existiert ein Referentenentwurf zum NIS-2-Umsetzungs-und Cybersicherheitsstärkungsgesetz[2] („NIS-2UmsuCG“), mit dem die Vorgaben in Deutschland umgesetzt werden sollen. Das Gesetz soll im März 2024 fertig sein und im Oktober 2024 in Kraft treten.

2. NIS-2 – Gibt’s da noch was anderes?

Die NIS-2 ist Teil einer ganzen Reihe neuer Rechtsetzungsakte der EU-Kommission im Rahmen der EU-Cybersicherheitsstrategie[3].

Der **Digital Operational Resilience Act (DORA)** ist seit dem 17. Januar 2023 in Kraft und muss bis zum 17. Januar 2025 umgesetzt werden. Er gilt ergänzend zur NIS-2 RL bzw. deren nationalen Umsetzungsgesetzen und soll als Verordnung unmittelbar zur Stärkung der IT-Sicherheit von Finanzunternehmen führen. DORA stellt einheitliche Anforderungen für die Sicherheit von Netzwerk- und Informationssystemen, die die Geschäftsprozesse von Finanzunternehmen unterstützen. Bezweckt wird insbesondere die Vereinheitlichung der Vorgaben zur IT-Sicherheit, Verankerung auf Gesetzesebene sowie die Schließung von Lücken und Behebung von Unstimmigkeiten in einigen der vorausgehenden Rechtsakte.

DORA ist gegenüber der NIS-2 ein *lex specialis*. Sie gilt also vorrangig und enthält strengere Maßstäbe als die NIS-2 u.a. an IKT-Risikomanagement und Meldungen von IKT-Vorfällen.

Der **Cybersecurity Act**[5] **(CSA)** ist am 27.06.2019 in Kraft getreten und hat die nationalstaatenübergreifende Zertifizierung von Cybersicherheit von Produkten zum Ziel. Damit soll Cyberattacken präventiv vorgebeugt werden. Zudem sollen wettbewerbsrechtliche Anreize für Unternehmen, in die Cybersicherheit ihrer Produkte zu investieren, geschaffen werden.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (aufgerufen am 23.10.2023).

[2] https://ag.kritis.info/wp-content/uploads/2023/07/NIS2UmsuCG-Referentenentwurf-BMI-CI1-Bearbeitungsstand-03072023.pdf (heruntergeladen am 23.10.2023).

[3] https://digital-strategy.ec.europa.eu/de/policies/cybersecurity-strategy (aufgerufen am 24.10.2023).

[4] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (aufgerufen am 24.10.2023).

[5] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881 (aufgerufen am 24.10.2023).

Teil der Cybersicherheitsstrategie ist auch der **Cyber Resilience Act**[6] **(CRA)**. Bislang existiert hierzu lediglich ein Vorschlag der EU-Kommission vom 15.09.2022. Der CRA bezweckt die Einführung von Sicherheitsanforderungen für ein breites Spektrum an Produkten mit digitalen Elementen und ergänzt bestehende Regelungen mit produktbezogenen Vorgaben.

Die **Critical Entities Resilience Richtlinie**[7] **(CER)** geht auf ein EU-Regelwerk zur IT-Sicherheit kritischer Infrastrukturen zurück, das bereits viele Jahre vor der NIS-Richtlinie galt. Die CER aktualisiert diese Regeln und beinhaltet Mindestanforderungen für die Resilienz kritischer Infrastrukturen in der EU. Die CER steht quasi neben der NIS-2, hat jedoch einen deutlich engeren Anwendungsbereich. Sie wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht und ist bereits in Kraft. Die Umsetzung in nationales Recht hat bis zum 17. Oktober 2024 zu erfolgen. In Deutschland wird sie mit dem KRITIS-Dachgesetz, wahrscheinlich ab 2024, umgesetzt. Sowohl das KRITIS-Dachgesetz als auch das NIS-2-UmsuCG erweitern die IT-Sicherheits-Regulierung für Unternehmen und sonstige betroffene Organisationen deutlich in Breite und Tiefe. Die Schnittstellen zwischen den beiden Bereichen sollen im Rahmen der Umsetzung angeglichen und soweit möglich übereinstimmend geregelt werden.

3. Für wen gilt die NIS-2?

Die auf der NIS-2 basierenden mitgliedsstaatlichen Vorgaben gelten für eine deutlich größere Gruppe an Organisationen, als dies unter bisheriger Rechtslage der Fall war. Der Anwendungsbereich wurde somit erheblich ausgeweitet. Die Ausweitung des Anwendungsbereichs wird insbesondere dadurch erreicht, dass bei der Bestimmung betroffener Unternehmen „nur" noch nach Zugehörigkeit zu einem Geschäftsfeld bzw. wirtschaftlicher Tätigkeit („Sektoren") und der Unternehmensgröße nach Mitarbeiteranzahl und Umsatz unterschieden wird.

Die NIS-2 gilt für Organisationen, die in bestimmten Sektoren tätig sind, die sich aus den Anlagen I und II zur NIS-2 ergeben. Unterschieden wird zwischen „wesentlichen" und „wichtigen" Einrichtungen. Die Unterscheidung ist für den Umfang der staatlichen Aufsicht und die Sanktionsmöglichkeiten von Bedeutung.

Zu den **wesentlichen Einrichtungen** (Anhang I) zählen: Energie, Transport, Banken, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, ICT-Dienstleistungsverwaltung, Raumfahrt, öffentliche Verwaltung.

Wichtige Einrichtungen (Anhang II) umfassen: Post und Kurier, Abfallwirtschaft, Chemie, Lebensmittel, Industrie, digitale Dienste, Forschung.
Betroffen sind öffentliche und private Einrichtungen, die als mittlere und große Unternehmen im Sinne der 2003/361/EG gelten, also gewisse Schwellenwerte überschreiten, sog. „size-cap-Regel". Unabhängig von der Größe gilt sie für besonders kritische Dienste, Art. 2 Abs. 2.

Große Unternehmen sind solche mit mehr als 250 Beschäftigten und einem Jahresumsatz von mehr als 50 Mio. Euro oder einer Jahresbilanz von mehr als 43 Mio. Euro.

Mittlere Unternehmen sind solche mit weniger als 250 Beschäftigten und einem Jahresumsatz von höchstens 50 Mio. Euro oder einer Jahresbilanz von maximal 43 Mio. Euro.

Abzugrenzen sind mittlere von **kleinen und Kleinstunternehmen**, für die die NIS-2 Vorgaben grundsätzlich nicht gelten, es sei denn, besondere Ausnahmen liegen vor. Kleine Unternehmen sind solche, die weniger als 50 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 10 Mio. Euro nicht übersteigt. Kleinstunternehmen sind solche, die weniger als 10 Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz 2 Mio. Euro nicht überschreitet.

Solche Organisationen können ausnahmsweise den NIS-2 Vorgaben unterfallen, wenn sie besonderen Sektoren zuzuordnen sind (z.B. Betreiber von Kommunikationsnetzen) oder besondere Gefahrenlagen bestehen (u.a. im Bereich der öffentlichen Ordnung und Sicherheit, wesentliche Systemrisiken, bestimmte öffentliche Verwaltungsbereiche; vgl. Art 2 Abs. 2).

[6] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0404 (aufgerufen am 24.10.2023).

[7] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557 (aufgerufen am 24.10.2023).

4. Welche Anforderungen bringt die NIS-2?

Die Stärkung der Cyberresilienz von betroffenen, überwiegend privatwirtschaftlichen Unternehmen steht im Vordergrund der NIS-2. Die NIS-2 enthält eine Reihe von strengeren Cyber-Risikomanagement-Anforderungen, die sich für wesentliche und wichtige Einrichtungen nicht wesentlich unterscheiden. Insbesondere wird die Verantwortlichkeit der Leitungsorgane erheblich ausgeweitet. Die wesentlichsten Regelungen werden nachfolgend kursorisch dargestellt, um einen ersten groben Überblick zu liefern, der dann mit einer detaillierteren Lektüre der vollständigen Regelungen der NIS-2 und der jeweiligen Umsetzungsregelungen vertieft werden kann und sollte.

Risikomanagementmaßnahmen (Art. 21)

Zum einen sind angemessene technische und organisatorische Maßnahmen (TOM) zu ergreifen, die die folgenden Maßnahmen, Konzepte und Prozesse umfassen müssen, die zudem je nach Größe, Risiken und Ausmaß der Gefährdung individuell anzupassen sind:

- Risikoanalyse und Sicherheit für Informationssysteme,
- Bewältigung von Sicherheitsvorfällen,
- Aufrechterhaltung des Betriebs einschl. Backup-Management und Wiederherstellung nach Notfällen sowie Krisenmanagement,
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleanbietern,
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,
- Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung,
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Berichtspflichten (Art. 23)

Über jeden erheblichen Sicherheitsvorfall ist grundsätzlich innerhalb von 24 Stunden zu berichten. Die Information hat gewisse Mindeststandards zu erfüllen und erfolgt danach gestuft nach bestimmten zeitlichen Vorgaben (u.a. mit Zwischen- und Abschlussberichten an die zuständigen Behörden). Potenziell von einer erheblichen Cyberbedrohung betroffene Nutzer sind unter gewissen Umständen unverzüglich über die erhebliche Cyberbedrohung sowie Maßnahmen bzw. Abhilfemaßnahmen zu informieren, die als Reaktion auf die Bedrohung ergriffen werden können.

Governance (Art. 20)

Leitungsorgane haben die Umsetzung der zu ergreifenden Risikomanagementmaßnahmen zu überwachen und können für Verstöße verantwortlich gemacht werden. Sie müssen an Schulungen teilnehmen und dafür Sorge tragen, dass diese regelmäßig für alle Mitarbeiter angeboten werden.

Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung (Art. 24)

Die Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten spezielle IKT-Produkte, Dienste und -Prozesse zu verwenden, die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung gemäß Artikel 49 der Verordnung (EU) 2019/881 zertifiziert sind, um die Erfüllung bestimmter Anforderungen nachzuweisen.

5. Welche Befugnisse bekommen Behörden und was passiert bei Verstößen?

Artt. 32 und 33 beinhalten Vorgaben zu Regelungen von Durchsetzungsbefugnissen der zuständigen Behörden sowie Fälle von Rechtsverstößen.

Aufsichtsmaßnahmen und Befugnisse

Folgende Aufsichtsmaßnahmen und Durchsetzungsbefugnisse seitens der zuständigen Behörden sind vorgesehen:

Für wesentliche Einrichtungen:

- Vor-Ort-Kontrollen, Tests, Audits;
- regelmäßige und gezielte Ad-hoc-Security-Audits,
- Sicherheitsscans,
- Anforderung von Informationen, Nachweise und Zugang zu Daten über die ergriffenen Risikomanagementmaßnahmen und solchen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind,
- Warnungen und verbindliche Anweisungen, dass gegen die NIS-2 verstoßende Verhalten einzustellen und von Wiederholungen abzusehen ist,
- Bestellung eines Aufsichtsbeamten und
- Verhängung einer Geldbuße.

Bei fortwährender Non-Compliance sollen Behörden Fristen setzen können, innerhalb derer die erforderlichen Maßnahmen ergriffen werden müssen. Bei nicht fristgemäßer Umsetzung ist der vorübergehende Entzug der Betriebserlaubnis, Zertifizierungen o.ä. möglich, sowie die vorübergehende Untersagung

der Wahrnehmung von Führungsaufgaben durch das Führungsorgan.

Für wichtige Einrichtungen:

Hinsichtlich der Aufsichtsmaßnahmen und Durchsetzungsbefugnisse der Behörden bestehen zwischen wesentlichen und wichtigen Einrichtungen kaum Unterschiede.

Ein Unterschied besteht lediglich darin, dass die zuständigen Behörden bei der Unwirksamkeit einer Maßnahme nicht nach Art. 32 Abs. 5 befugt sind eine Frist zur Umsetzung der Maßnahmen festzusetzen und bei der Nichtumsetzung auch keine weiteren Maßnahmen ergreifen können (z.B. Aussetzung der Zertifizierung oder Untersagung der Wahrnehmung von Führungsaufgaben der Führungsorgane).

Sanktionen

Wesentlichen Einrichtungen droht unter mitgliedstaatlichen Regelungen ein Bußgeld von bis zu 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist. Bei wichtigen Einrichtungen können Bußgelder bis zu 7 Mio. Euro oder 1,4% des weltweiten Jahresumsatzes verhängt werden, je nach dem welcher Betrag höher ist. Die Vorgaben können im Rahmen der Umsetzung noch verschärft werden, was u.a. in Deutschland geplant ist (bis zu 20 Mio. Euro bzw. 2% des weltweiten Jahresumsatzes).

Die persönliche Verantwortlichkeit von Führungsorganen und anderen Leitungsorganen wird erheblich verschärft. Neben der Möglichkeit der vorübergehenden Untersagung der Wahrnehmung von Führungsaufgaben haften Führungsorgane für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung der NIS-2 persönlich. Der Verzicht der Organisation auf Ersatzansprüche gegen die Geschäftsleitung oder ein entsprechender Vergleich sollen unwirksam sein.

6. Was Unternehmen jetzt tun müssen

Die Regelungen zur NIS-2 sind bereits auf dem Weg und werden auf absehbare Zeit auch in Deutschland gelten. Sie werden – anders als früher – eine deutlich größere Anzahl von Unternehmen und Organisationen erfassen und bringen deutlich striktere Vorgaben an das Management von Cyberrisiken und die Governance in der Organisation.

Unternehmen sollten in einem ersten Schritt prüfen, ob und wenn ja in welchem Umfang die zukünftigen Regelungen relevant sind. Eine solche Prüfung lässt sich heute bereits gut anhand der Regelungen der NIS-2 und der Schwellenwert- und Sektorenanalyse durchführen. Finden die Regelungen danach zukünftig Anwendung ist zeitnah eine erste GAP-Analyse zwischen den aktuell bestehenden Konzepten, Policies und Prozessen und dem zukünftigen Zielbild durchzuführen, um möglichst zeitnah mit ersten Vorbereitungen und Anpassen beginnen zu können. Besonderes Augenmerk sollte auf das Management von Drittparteirisiken (Stichwort „Lieferkette“) sowie die erweiterten Verantwortlichkeiten der Geschäftsleitung gelegt werden, um rechtzeitig adäquate Maßnahmen und Prozesse zur Risikosteuerung umsetzen zu können. Im Rahmen der Umsetzung sind etwaige Änderungen und Verschärfungen im Rahmen der nationalen Umsetzung zu verfolgen, um die eigenen Konzepte zeitnah an entsprechende Änderungen anpassen zu können.

Und wie immer gilt: Zeitnah loslegen, denn die Zeit zur Umsetzung der Regelungen ist knapp bemessen!

Über die Autoren

Thomas Kahl
Fachanwalt für IT-Recht, Taylor Wessing
Der Autor berät nationale wie internationale Unternehmen zu allen Fragen des Datenschutz- und IT-Sicherheitsrechts sowie datenschutzrechtlichen Streitigkeiten und aufsichtsbehördlichen Verfahren.

Teresa Kirschner
ist Rechtsanwältin und im TMT-Team der internationalen Wirtschaftskanzlei Taylor Wessing am Standort Frankfurt am Main tätig.

▶ www.taylorwessing.com

TaylorWessing

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, Dagmar Hartge

PORTALE, REGISTER, PLATTFORMEN

Internationales Symposium bei der Aufsichtsbehörde Brandenburg.

Sven Müller

Portale, Register, Plattformen – digital und transparent?

Bereits seit dem Jahre 1999 veranstaltet die brandenburgische Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in jedem zweiten Jahr ein Internationales Symposium in Potsdam. Es befasst sich mit den Themen Informationsfreiheit und Transparenz. In diesem Jahr stand Open Data auf der Tagesordnung; der Titel der Veranstaltung lautete „Portale, Register, Plattformen – digital und transparent?“ Für den 16. Oktober 2023 lud die Landesbeauftragte Expertinnen und Experten aus verschiedenen europäischen Ländern nach Potsdam ein, um ihre Erfahrungen vorzustellen und gemeinsam mit einem interessierten Publikum zu diskutieren. Einer Dokumentation der Veranstaltung soll an dieser Stelle auch aus Platzgründen nicht vorgegriffen werden. Einige Erkenntnisse aus den Präsentationen sowie aus der abschließenden Podiumsdiskussion lassen sich aber auch ableiten, ohne die einzelnen Vorträge im Detail wiederzugeben:

Europäische Dimension

Zunächst muss die europäische Dimension von Open Data betont werden. Dies betrifft sowohl die praktische Seite, also beispielsweise das Portal data.europa.de der Europäischen Kommission sowie deren Open-Data-Strategie, als auch die rechtlichen Grundlagen. So zeigte Slowenien auf, dass man sich dort bereits frühzeitig an europarechtlichen Vorgaben orientierte und die novellierten Richtlinien und Verordnungen als Richtschnur berücksichtigte.

Die Europäische Kommission selbst bietet neben dem genannten Portal auch umfangreiche Informationen zu Open Data sowie Kurse und Webinare an. Mit ihrem „Open Data Maturity assessment“ bewertet sie die Fortschritte der Umsetzung in den Mitgliedstaaten sowie darüber hinaus und veröffentlicht die Ergebnisse in einem jährlichen Bericht. Gerade auf europäischer Ebene leuchtet das Erfordernis eines funktionierenden und bis in die Datensätze selbst hineinwirkenden Übersetzungs-Tools unmittelbar ein.

Daten und Metadaten

Deutlich wurde, dass es nicht darum geht, Daten zwischen den Portalen und Plattformen zu transferieren, sondern lediglich die zugehörigen Metadaten. Portale fungieren also meist als Metadatenkataloge. Voraussetzung ist, dass überall dieselben Standards eingehalten und Schnittstellen eingerichtet werden, die beispielsweise ein automatisiertes Harvesting ermöglichen. Neben der technischen Interoperabilität muss aber auch die Qualität der Daten gewährleistet und ihre Beschreibung in den Metadaten möglichst einheitlich strukturiert sein. Eine Qualitätssicherung kann mit eigenen Mitteln oder auch unter Einbeziehung der Zivilgesellschaft erfolgen, beispielsweise zum Zweck der Validierung. Je flexibler die Ausgabeformate der Plattformen sind, umso umfangreicher können Nutzerinnen und Nutzer die Daten einsetzen. Und so simpel es klingt: Informationen müssen überhaupt erst in Form digitaler Daten vorhanden sein. Bei der Frage, welche Daten für die Öffentlichkeit interessant sind, ließ sich eine deutliche Tendenz erkennen: Grundsätzlich alle, jedenfalls trifft die Verwaltung nur selten

ins Schwarze, wenn sie versucht, ein öffentliches Interesse zu antizipieren. Eine möglichst offene Lizenzierung der Daten versteht sich im Sinne des Weiterverwendbarkeitsgebots von selbst.

Erfolgsfaktor Vernetzung

Selbst wenn offene Daten in großem Umfang auf Portalen und Plattformen zur Verfügung gestellt werden, ist Open Data keineswegs ein Selbstläufer. Innerhalb der Daten haltenden Stellen bedarf es einer organisatorischen Struktur – beispielsweise Open-Data-Beauftragter oder „Stewards", die sich untereinander vernetzen. Auch den Aufbau einer Open-Data-Community sahen die Expertinnen und Experten als unabdinglich an.

Aus Estland war zu erfahren, dass dort besonders die kleineren Kommunen mit großem Engagement von der Sinnhaftigkeit offener Daten überzeugt werden. Das zuständige Ministerium leistet dort teilweise kleinteilige Unterstützung und hat sich landesweit zum Hauptansprechpartner für die Umsetzung von Open Data entwickelt.

Überzeugungsarbeit hat hier erste Priorität; Aufsichtsmaßnahmen können nur Ultima Ratio sein. In mehreren Beiträgen wurde deutlich, dass gerade der öffentliche Sektor häufig intensiver Nutzer der Portale und Plattformen ist. Die Behörden haben somit selbst einen Vorteil davon, sich an Open Data zu beteiligen. In Slowenien gehören zu der Open-Data-Community neben den öffentlichen Verwaltungen auch Bildungseinrichtungen, Forschungsinstitute, Nichtregierungsinstitutionen, investigative Journalistinnen bzw. Journalisten sowie Unternehmen der digitalen Wirtschaft – vom Startup bis zum Konzern. Das Portal selbst stellt dabei das Rückgrat dieses Datenangebots dar. Innerhalb der Community geht es darum, das Engagement der teilnehmenden Einrichtungen zu fördern, beispielsweise durch Wettbewerbe und Best-Practice-Ausschreibungen.

Aufbereitung und Visualisierung

Neben diesen eher organisatorischen Gesichtspunkten sehen die Betreiberinnen und Betreiber von Portalen und Plattformen zunehmend die Bereitstellung von Auswertungen als ihre Aufgabe an. Häufig wurde betont, wie wichtig es sei, Daten so zu visualisieren, dass sie nicht nur neue Erkenntnisse bringen, sondern zudem leicht zu verstehen sind. Die Zusammenarbeit mit Grafikerinnen und Grafikern oder auch mit Datenjournalistinnen und Datenjournalisten ist hier hilfreich. Aus Rohdaten können plattformenübergreifend verständliche Informationen werden. Die Europäische Umweltagentur kombiniert zum Beispiel Daten aus der Erdbeobachtung, also Geodaten, mit solchen aus der Umweltstatistik. Daraus entstehen anschauliche Kartenanwendungen, die sowohl für Bürgerinnen und Bürger sowie Umweltorganisationen als auch für Entscheidungsträgerinnen und Entscheidungsträger in Politik und Verwaltung aus sich heraus verständlich sind.

Stärkung der Demokratie

Die niederländische Open State Foundation setzt sich für digitale Transparenz ein, indem sie öffentliche Informationen in Form von offenen Daten zugänglich macht und für die Weiterverwendung bereitstellt. Ihr Ziel ist es, bürgerschaftliches Engagement und demokratische Teilhabe zu fördern. Einen Gegensatz zwischen Gesellschaft und Regierung sieht sie nicht. Sie versteht sich selbst als „Rebel and partner". In Zusammenarbeit mit dem Innenministerium entsteht in den Niederlanden gerade ein Contract Register, das neben Beschaffungsdaten auch Verträge in umfassender Weise beinhalten soll – das Projekt wird im Übrigen auch von den betroffenen Unternehmen befürwortet. Auch andere „Open State Tools" stellt die Open State Foundation bereit, so beispielsweise zum Einfluss der Lobbys, zum Eigentum an Unternehmen und zu Finanzdaten der öffentlichen Hand. Den Medien kommt bei der Vermittlung der

(aufbereiteten) Erkenntnisse aus den bereitgestellten Daten eine Schlüsselrolle zu.

Open Data im Föderalismus

Anhand des deutschen Portals GovData lässt sich erkennen, welche Herausforderung neben der sektoralen zusätzlich die föderale Gliederung von Portalen und Plattformen darstellt. Inzwischen sind alle Bundesländer der Vereinbarung, auf deren Grundlage GovData betrieben wird, beigetreten. Auf der Ebene der Regierungsbezirke, Landkreise, Städte und Gemeinden bestehen jedoch noch immer erhebliche Lücken – sowohl in der Beteiligung an dem Portal als auch im Umfang, der Strukturiertheit und Qualität der eingespeisten Daten. So böten 39 Prozent der Kommunen ihre Daten ausschließlich zum Download auf der eigenen Webseite an, und 36 Prozent ohnehin nur individuell auf Anfrage. Ein Harvesting der europäischen bzw. Bundesebene bis hinunter auf die kommunalen Plattformen muss unter diesen Voraussetzungen ziemlich lückenhaft bleiben. Inwieweit das auf Bundesebene geplante Transparenzgesetz einen Rechtsanspruch auf Open Data beinhalten wird, ist derzeit noch offen. Entscheidend wird sein, dass auf allen Ebenen eine ausreichende und vor allem kompatible informationstechnische Infrastruktur sowie finanzielle und personelle Ressourcen für Open Data bereitstehen.

Informationsfreiheit und Open Data

Offen blieb die Frage nach dem Verhältnis zwischen der klassischen Informationsfreiheit und Open Data: Lange war die Trennlinie klar definiert: Informationsfreiheit betrifft unstrukturierte Informationen, also solche, die klassischerweise in Textform für den Menschen verständlich sind, während sich Open Data auf strukturierte, maschinenlesbare Rohdaten bezieht, die erst einer Aufbereitung bedürfen, bevor sie in einer vergleichbaren Weise wie Texte verständlich werden. Es fragt sich, ob diese Trennung angesichts der flächendeckenden Einführung der E-Akte, der zunehmenden Umsetzung von Vorschriften über die Barrierefreiheit und der Möglichkeiten künstlicher Intelligenz überhaupt noch aufrechtzuerhalten ist. Für eine zunehmende Unschärfe spricht, dass Auswertungen offenbar nicht mehr nur der unsichtbaren Hand des Datenmarktes überlassen, sondern von Plattformen selbst übernommen oder zumindest initiiert werden.

Zentral oder dezentral?

Auch wenn der Begriff „Data hub“ häufig positiv konnotiert fiel, fand sich keine eindeutige Antwort darauf, in welchem Verhältnis zentrale Portale und dezentrale Plattformen zueinander stehen. Ist es sinnvoller, möglichst viele derzeit in föderal wie sektoral unterschiedlichen Portalen vorhandenen Informationen und Daten in ein zentrales Portal zu überführen, und sei es nur durch die Zusammenführung der Metainformationen? Oder würde darunter die Übersichtlichkeit und Auffindbarkeit der Daten leiden?

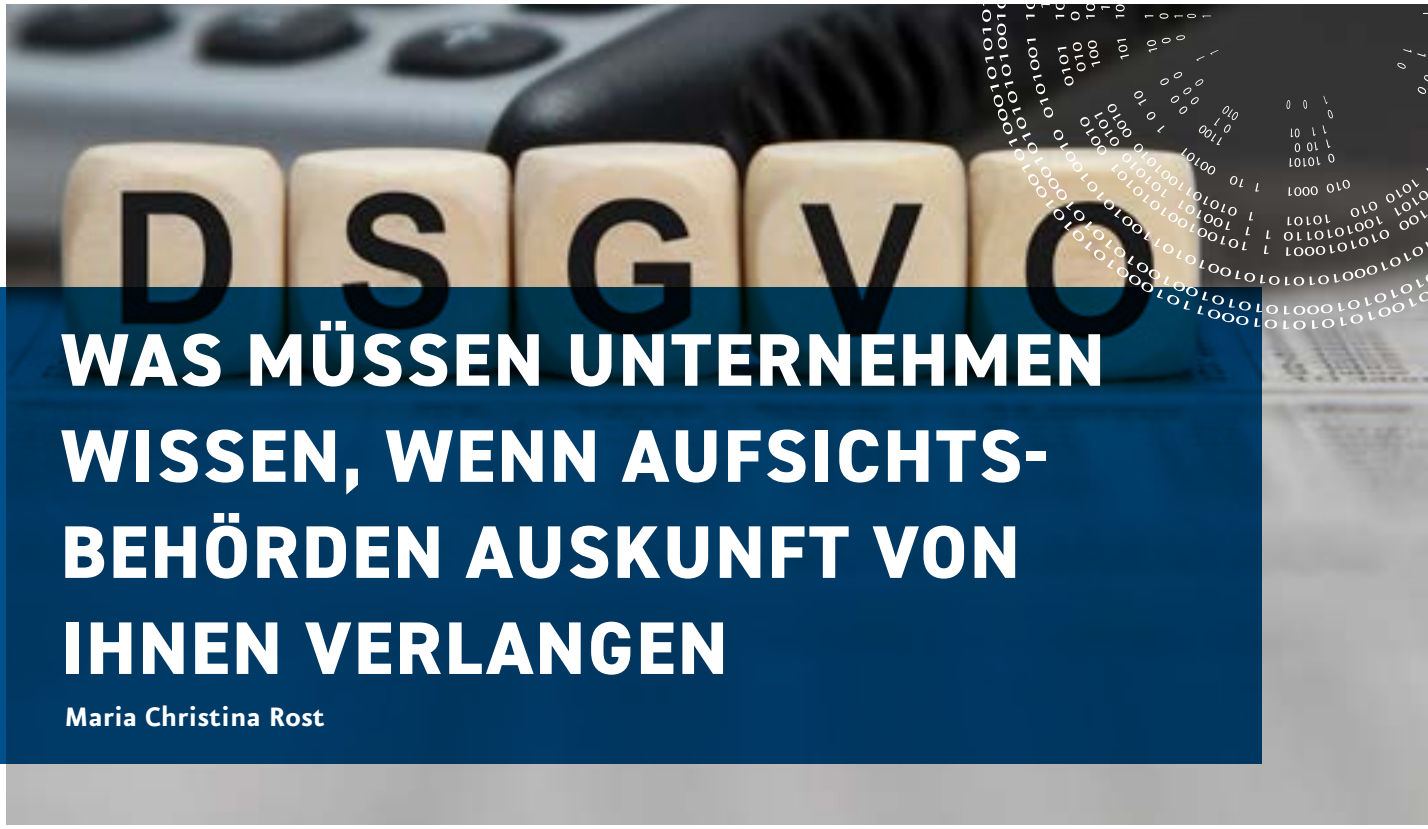
AUSBLICK: KÜNSTLICHE INTELLIGENZ

Die Rolle des metaphorischen „Elephant in the room“ übernahm während des gesamten Internationalen Symposiums die künstliche Intelligenz. Aus den Vorträgen ging hervor, dass entsprechende Instrumente bereits Anwendung finden, deutlich wurde aber vor allem, dass künstliche Intelligenz nur soweit reicht wie die Daten, die ihr zur Verfügung stehen. Es wäre sicher keine Überraschung, wenn eine der nächsten Veranstaltungen aus dieser Reihe sich dieser Thematik widmen würde.

Über den Autor

Sven Müller
ist Referent für Informationsfreiheit bei der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht in Brandenburg. Das Internationale Symposium hat er seit Beginn dieser Veranstaltungsreihe im Jahre 1999 begleitet.

▶ https://www.lda.brandenburg.de/



WAS MÜSSEN UNTERNEHMEN WISSEN, WENN AUFSICHTS-BEHÖRDEN AUSKUNFT VON IHNEN VERLANGEN

Maria Christina Rost

Anforderungen an ein Auskunftsverlangen der Aufsichtsbehörde (Art. 58 DSGVO)[1]

Der Verantwortliche, der Auftragsverarbeiter oder Vertreter der beiden in der Verantwortung – Was kommt auf ihn zu?

Der Datenschutzaufsichtsbehörde (im Folgenden Aufsicht/Behörde) stehen durch die DS-GVO verschiedene Handlungsmöglichkeiten zur Verfügung, um an die notwendigen Informationen zu kommen, die es ihr ermöglichen, ihre Aufgaben nach Art. 57 DS-GVO zu erfüllen. Für die verantwortliche Stelle und den Auftragsverarbeiter ist es hilfreich, diese Optionen zu kennen, damit er sein Datenschutz-Compliance hierauf anpassen kann.

Überblick

Um die Einhaltung der DS-GVO zu überwachen und durchzusetzen, muss die Aufsicht zunächst den Sachverhalt im erforderlichen Umfang ermitteln. Das Handeln der Aufsicht richtet sich nach den nationalen Verfahrensvorschriften (s. Art 58 Abs. 4 DS-GVO). Dies sind unter anderem die Vorschriften des Verwaltungsverfahrensgesetzes (VwVfG) und des Verwaltungsvollstreckungsgesetzes (VwVG) des Bundes und der Länder. Für die Sachverhaltsermittlung der Datenschutzaufsichtsbehörde gilt der Amtsermittlungsgrundsatz nach § 24 VwVfG. Nach § 24 Abs. 1 Satz 1 und 2 VwVfG ermittelt die Behörde den Sachverhalt von Amts wegen. An das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden. Sie bestimmt Art und Umfang der Ermittlungen. Dabei hat sie nach § 24 Abs. 2 VwVfG alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände, zu berücksichtigen.

Beschwert sich beispielsweise ein Bürger bei der Aufsicht über ein Unternehmen, über Videokameras, wird sie dieses Unternehmen in der Regel unter Fristsetzung zur Stellungnahme auffordern. Oftmals geschieht dies im Zusammenhang mit der Zusendung eines Fragenkataloges. Dies ist insbesondere in Standardfällen der Fall, wie z.B. der Videoüberwachung. Die Fristsetzung dient dabei der Förderung des Verfahrens. Dieses allgemeine Informationsverlangen, ist durch die Aufgabenzuweisung in Art. 57 DS-GVO i.V.m. mit den national zugewiesenen Aufgaben und durch die Befugnisse in Art. 58 DS-GVO gedeckt. Dabei ist bei Beschwerdeverfahren i.S.d. Art. 77 DS-GVO zu berücksichtigen, dass die Aufsicht innerhalb von drei Monaten i.S.d. Art. 78 Abs. 2 DS-GVO gegenüber dem Bürger eine Stellungnahme abzugeben hat. In das informelle Auskunftsersuchen wird die Aufsicht in der Regel zwei Normen hineinschreiben. Zum einen wird sich die Aufsicht sich auf Art. 31 DS-GVO berufen und auf § 40 Abs. 4 S. 1 BDSG. Art. 31 DS-GVO hinweisen[2]. Neben dem allgemeinen Informationsverlangen gibt es spezifische Informationsverlangen. Hierunter zählen insbeson-

[1] Die Verfasserin vertritt ihre persönliche Auffassung, die nicht notwendigerweise der Auffassung des Dienstherrn entspricht.

[2] S. auch Erwägungsgrund 82 zur DS-GVO.

dere die Vorlage des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 Abs. 4 DS-GVO). Nach Erwägungsgrund 82 Satz 1 bedeutet dies, dass der Verantwortliche oder der Auftragsverarbeiter zum Nachweis der Einhaltung dieser Verordnung ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen sollte. Ein weiteres spezifisches Auskunftsverlangen ergibt sich aus der Pflicht zur Dokumentation der „Sicherheitspannen" (Art. 33 Abs. 5 S. 2 DS-GVO).

Führt das allgemeine oder spezifische Informationsverlangen nicht zum Ziel, wird die Aufsicht durch ihre Untersuchungsbefugnisse nach Art. 58 Abs. 1 DS-GVO in die Lage versetzt, die Information förmlich anzufordern und dies mit Maßnahmen des Verwaltungszwangs (nach VwVG), wie beispielsweise der Androhung und später der Festsetzung von Zwangsgeld, zu begleiten. Die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO ist keine Regelung zur Vorlage bei der Aufsichtsbehörde, aber sie regelt das „Nachweisen können". Sie ist ein Sonderfall der Rechenschaftspflicht.

Zusammenarbeit mit der Aufsichtsbehörde - Art. 31 DS-GVO

In der Regel wird die Aufsichtsbehörde sich mit einer informellen Auskunftsanforderung beim Verantwortlichen, Auftragsverarbeiter oder Vertreter melden. In diesen Schreiben ist in der Regel eine Aufforderung zur Zusammenarbeit mit Hinweis auf Art. 31 DS-GVO und § 40 Abs. 4 BDSG finden. Der Art. 31 DS-GVO hat in den ersten Jahren der fünf Jahre DS-GVO ein Nischendasein geführt. Mittlerweile wird er immer häufiger von der Aufsicht ins Spiel gebracht und führt auch zur Verhängung von Geldbußen. Nach Art. 31 DS-GVO arbeiten der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter auf Anfrage mit der Aufsicht bei der Erfüllung ihrer Aufgaben zusammen. Es ist eine Pflicht zur Zusammenarbeit, die sich im Grunde nach schon aus Art. 58 Abs. 1 DS-GVO herleiten lässt.

Dadurch entsteht aber auch ein Spannungsfeld zwischen den Interessen des Auskunftspflichtigen und den Interessen der Aufsicht. Dem Spannungsfeld zwischen dem Verbot der Selbstbezichtigung und dem Amtsermittlungsgrundsatz wird dadurch Rechnung getragen, dass die Ausübung der Befugnisse den allgemeinen innerstaatlichen Voraussetzungen an die Rechtmäßigkeit eines Verwaltungsaktes gebunden ist. Die Aufsicht muss die Anforderung auf Zusammenarbeit konkretisieren. Die Verpflichtung umfasst zur Zusammenarbeit erfasst auch Betriebs- und Geschäftsgeheimnisse. Diese sind aber entsprechend von der Aufsicht zu schützen (z.B. Schwärzung) und nicht weiterzugeben. Kritisch zu hinterfragen ist die Pflicht zur Zusammenarbeit mit der Aufsicht bei Anfragen derselben ohne konkreten Anlass, solche Anfragen, die „ins Blaue" hineingehen.

Die Aufsicht kann nur verlangen, was für die Erfüllung der Aufgaben für erforderlich gehalten wird. Hierzu muss die Behörde konkretisieren, welche Informationen sie benötigt, um eine Entscheidung treffen zu können. Aufgrund einer unklaren Sachlage, die beispielsweise durch eine eingereichte Beschwerde entsteht, kann es sein, dass die Datenschutzaufsicht sich an den zugrundeliegenden Sachverhalt langsam in mehreren Schritten annähern muss.

Auskunftsanordnung und Mitwirkungspflicht

Führt die informelle Auskunftsanfrage nicht zum Erfolg, kann die Aufsicht die Auskunft auch anweisen (Art. 58 Abs. 1 lit. a DS-GVO). Ziel der Aufsicht ist auch hierbei immer die Aufgabenerfüllung i.S.d. Art. 57 DS-GVO und möglicher weiterer Aufgaben. Davon zu trennen ist die Auskunft nach Art. 15 DS-GVO.

Art. 58 Abs. 1 DS-GVO eröffnet jeder Aufsicht Untersuchungsbefugnisse, die es ihr gestatten, den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls deren Vertreter anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind (Art. 58 Abs. 1 lit. a DS-GVO), oder Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen (Art. 58 Abs. 1 lit. b

DS-GVO), sowie von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen zu verlangen, die zur Erfüllung ihrer Aufgaben notwendig sind (Art. 58 Abs. 1 lit. e DS-GVO).

Selbst bei der Anordnung einer solchen Untersuchungsmaßnahme sind die inhaltlichen Grenzen des Auskunftsverlangens zu wahren. Es sollte keine Ausforschung „ins Blaue hinein" stattfinden. Es sollte aber auch nicht Vagheit der Auskunft mit der Vagheit des Verlangens korrelieren. Besser ist es in solchen Fällen, mit der Datenschutzaufsicht ins Gespräch zu kommen.

Die Anordnung durch die Aufsicht ist ein Verwaltungsakt (s. § 35 VwVfG). Die Anordnung muss so konkret sein, dass der Verwaltungsakt inhaltlich hinreichend bestimmt (§ 37 Abs. 1 VwVfG) ist. Der Verpflichtete muss sein Handeln so einrichten können, dass er nicht gegen die Anordnung verstößt. Des Weiteren sollte der anordnende Bescheid auch eine Begründung enthalten (§ 39 Abs. 1 VwVfG), sofern keine Ausnahmen nach § 39 Abs. 2 VwVfG vorliegen. Zudem sollte er mit einer Rechtsbehelfsbelehrung versehen sein (§ 37 Abs. 6 VwVfG). Aber selbst wenn keine Rechtsbehelfsbelehrung darunter steht, kann es sich um einen Verwaltungsakt handeln. In diesem Fall verlängert sich die Klagefrist auf ein Jahr. Streitverfahren gegen die Verwaltungsakte werden vor dem jeweils zuständigen Verwaltungsgericht geführt.

Nach § 20 Abs. 1 i.V.m. Abs. 3 BDSG ist das Verwaltungsgericht örtlich zuständig, in dessen Bezirk die Aufsichtsbehörde ihren Sitz hat (z.B. Verwaltungsgericht Köln für Klagen gegen Entscheidungen des BfDI und Verwaltungsgericht Wiesbaden bei Klagen gegen Entscheidungen des HBDI).

Reagiert ein Unternehmen nicht auf das Auskunftsersuchen der Behörde nach Art. 58 Abs. 1 lit. a DS-GVO kann die Behörde auf Mittel des Verwaltungszwangs nach den Verwaltungsvollstreckungsgesetzen des Bundes und der Länder zurückgreifen. In der Regel wird auf das Zwangsgeld zurückgegriffen. Das Zwangsgeld ist keine Geldbuße. Es dient dazu, die Forderung aus dem Bescheid durchzusetzen. In einer ersten Stufe wird das Zwangsgeld angedroht. Dies geschieht in der Regel mit dem Erlass der Anweisung. Wird auf den Bescheid hin keine Auskunft erteilt, kann die Behörde das Zwangsgeld festsetzen. Die Höhe des Zwangsgeldes beträgt bis zu 25 000 Euro (§ 11 Abs. 3 VwVG). Führt die erste Anordnung eines Zwangsgeldes nicht zum Erfolg, kann bei der zweiten, dritten oder weiteren Anordnung ein höherer Betrag festgesetzt werden. Daher werden in der Regel auch nicht 25 000 Euro als erstes Zwangsgeld festgesetzt werden, sondern es wird eine Steigerungsmöglichkeit offengehalten.

Wahrung der „eigenen" Rechte des Auskunftspflichtigen

Kompliziert wird der Umgang mit Auskunftsverlangen der Aufsicht, wenn zum Beispiel seitens des Verantwortlichen oder Auftragsverarbeiter Pflichten nicht erfüllt wurden und dadurch die Bewertung der Lage erschwert wird.

Da fehlt es beispielsweise an der vorzulegenden Dokumentation oder an einer Datenschutz-Organisation. In diesen Moment wird es sinnvoll sein, sich von Anfang an eine Checkliste zu erarbeiten, die einem hilft die eigene Rolle zu bewerten (Verantwortlicher oder Auftragsverarbeiter), zu prüfen, ob Geheimhaltungspflichten von der Auskunft be-

troffenen sind, ob fremde Geschäftsgeheimnisse betroffen sind, ob ein Risiko dafür besteht, dass die Verarbeitung personenbezogener Daten datenschutzwidrig ist.

Bereits mit dem ersten Schreiben der Aufsicht, wird diese unter Hinweis auf das Aussageverweigerungsrecht (§ 40 Abs. 4 S. 1 BDSG) um Auskunft bitten. Die Behörde wird einen Bescheid verfassen, der unbestimmte, nicht erforderliche und unverhältnismäßige Fragen meidet, ebenso wie Fragen ins Blaue hinein. Besondere Aufmerksamkeit wird auch den Geschäftsgeheimnissen gewidmet werden, die eine Verschwiegenheitspflicht auslösen. Das in der Regel entstehende Spannungsverhältnis mit Blick auf Geschäftsgeheimnisse kann dazu führen, dass Unsicherheit entsteht, ob die Geschäftsgeheimnisse in der Auskunft aufgenommen werden sollten. Sinnvoll ist es, diese bei Übersendung als Geschäftsgeheimnisse zu markieren. Dann vermeidet man im Falle eines Akteneinsichtsgesuchs eines Betroffenen, sofern diese zulässig ist, langwierige Diskussionen.

Diese Probleme stellen sich immer häufiger, weil die Beschwerdeführer immer öfter auf der Suche nach Informationen für einen Zivilprozess gegen den Verantwortlichen sind und Schadensersatz nach Art. 82 DS-GVO geltend machen wollen. Da bereits im Aufsichtsverfahren Weichen für ein Bußgeldverfahren gestellt werden können, macht es zudem Sinn, die Wahrscheinlichkeit eines Bußgeldverfahrens auszuloten. Dabei ist zu berücksichtigen, dass bereits ein Verstoß gegen Art. 31 DS-GVO zu einem Bußgeld führen kann (s. Art. 83 Abs. 4 lit. a DS-GVO).

Rolle des Datenschutzbeauftragten

Adressaten der Pflichten nach Art. 58 Abs. 2 lit. a, 31 DS-GVO sind der Verantwortliche, der Auftragsverarbeiter und deren Vertreter. Der Datenschutzbeauftragte ist kein Adressat. Seine Rolle ergibt sich aus Art. 38 und 39 DS-GVO. Er hat den Verantwortlichen oder den Auftragsverarbeiter sowie die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. des Mitgliedstaates zu unterrichten und zu beraten (Art. 39 Abs. 1 lit. a DS-GVO). Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder Vertraulichkeit gebunden (Art. 38 Abs. 5 DS-GVO). Nach Art. 39 Abs. 1 lit. d DS-GVO arbeitet er mit der Aufsicht zusammen. Er steckt in einer Zwickmühle. Sowohl eine Auskunftserteilung als auch eine Nicht-Auskunft kann mit Risiken verbunden sein. Umso wichtiger ist es, die Rolle des Datenschutzbeauftragten gegenüber dem Unternehmen aus auch gegenüber der Aufsichtsbehörde klarzustellen[3].

Risiko Geldbuße

Oftmals verkennen die Unternehmen, dass Art 83 Abs. 4 und 5 DS-GVO Tatbestände enthalten, die mit dem Verhalten des Verantwortlichen oder des Auftragsverarbeiter im Aufsichtsverfahren mit der Untersuchung im Zusammenhang stehen. Nach Art. 83 Abs. 4 lit. a DS-GVO ist die Nichtbeachtung von Art. 31 DS-GVO bußgeldbewährt. Nach Art. 83 Abs. 5 lit. e DS-GVO ist die Nichtgewährung von Zugang i.S.d. Art. 58 Abs. 1 lit. e DS-GVO bußgeldbewährt. Darüber hinaus findet die Zusammenarbeit von Aufsichtsbehörde und Verantwortlichem oder Auftragsverarbeiter Berücksichtigung bei der Bußgeldbemessung (Art. 83 Abs. 2 lit. f DS-GVO). Dieses Risiko sollte von Anfang an im Auge behalten werden.

ZUSAMMENFASSUNG

Bittet die Aufsicht um Auskunft unter Hinweis auf Art. 31 DS-GVO und 40 Abs. 4 BDSG, dann beginnt hier schon die Frage, wie man mit diesem Auskunftsverlangen vernünftig umgeht. Der Dialog mit der Datenschutzaufsichtsbehörde kann helfen, bereits im frühen Stadium des Falls zu einem Ergebnis zu kommen. Auf ein unbeantwortetes Auskunftsschreiben folgt die Anweisung auf Auskunft nach Art. 58 Abs. 1 lit. a DS-GVO. Wenn das nicht beachtet wird, folgt die Anwendung von Verwaltungszwangsmitteln. Außerdem kann es unter anderem zur Verhängung von Geldbußen nach Art. 83 Abs. 4 lit. a DS-GVO kommen. Die bestehenden Spannungsverhältnisse gehen beide Seiten an und sollten gegenbenenfalls im Dialog mit der Aufsicht geklärt werden.

Über die Autorin

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

▶ https://datenschutz.hessen.de/

[3] Anfragen der Datenschutzaufsichtsbehörden: Auskunftspflicht oder nicht - So können Sie beraten!, Datenschutz-Praxis, Heft 06/2020, Seiten 1 bis 4.

ERIK MANKE

IDENTITÄTSDIEBSTAHL UND IDENTITÄTSMISSBRAUCH

„Identitätsdiebstahl“ ist das Schlagwort der letzten Jahre, wenn man sich die Betrugsszenarien in Deutschland anschaut.

Immer wieder und teilweise sogar organisiert angelegt, werden echte Identitätsdaten genutzt, um im E-Commerce Waren einzukaufen und Handyverträge abzuschließen. Ebenso werden Konsumentenkredite betrügerisch erlangt oder schlichtweg Bankkonten eröffnet, um diese sodann für Geldwäscheaktivitäten unterschiedlicher Couleur zu benutzen.

Aber: Wieso ist das so? Das war doch früher nicht so …?!?

Die Begründung dafür ist in der Tat relativ einfach erklärt:

Vor noch circa. 10 bis 15 Jahren konnten Betrüger unter Verwendung ausgedachter Personaldaten diese Betrugstaten begehen; also Personaldaten von Personen verwenden, die es tatsächlich gar nicht gibt. „Wie kann denn das sein?“ – mag man sich gerne und auch richtigerweise fragen. Im deutschsprachigen Raum gibt es die Zahlungsmethode „Kauf auf Rechnung“. Diese ist wesentlicher Bestandteil des Modus Operandi der Täter. Denn genau darum geht es: Sich als eine andere Person als sich selbst auszugeben und online Verträge abzuschließen. Die Rechnung erhält dann die Person, für die man sich ausgegeben hat. Bis vor den oben erwähnten 10 bis 15 Jahren konnten das Personaldaten sein, die es tatsächlich gar nicht gibt.

Die vertragsgegenständlichen Firmen haben dann jeweils versucht die „richtige“ Person ausfindig zu machen und haben dort die jeweilige Rechnung, Mahnung oder gar den Mahnbescheid zugestellt.

Aufgrund der Fülle der erfolgreichen Betrugstaten und massiven Anstiegs wurden Systeme entwickelt, die unter anderem die angegebenen Personaldaten auf Echtheit überprüfen.

Dies hatte zur Folge, dass der Warenkreditbetrug – so der Fachterminus – sehr erfolgreich bekämpft werden konnte. Der Erfolg währte jedoch nur kurz, da die Betrüger diese Präventionsmaßnahme schnell erkannten und umgingen, indem sie echte Personaldaten nutzen, um den Identitätsprüfungen standhalten zu können.

Um erkennen zu können, wie die Täter vorgehen, muss man sich zuerst Gedanken machen, welche Daten diese überhaupt brauchen. Je nach Deliktsbereich („Kauf auf Rechnung", „Mobilfunkvertragsbetrug" oder „Konsumentenkreditbetrug") sind dies nämlich unterschiedliche. Mal reichen „Vorname; Nachname, Wohnort" (= Stadt, oder Dorf), mal bedarf es der genauen „Wohnadresse" (also auch Straße und Hausnummer) und mal benötigt man dazu noch das Geburtsdatum, teilweise je nach Geschäftsgebahren des anvisierten zu betrügenden Vertragspartners, aber auch je nach gesetzlicher Bestimmung der Datenerhebung im Rahmen der Legitimationspflicht (wie beispielsweise beim Konsumentenkredit oder dem Mobilfunkvertrag).

Es wird schnell klar, dass es so ist, wie es eigentlich immer ist: „Je mehr Daten, desto besser!"

Ich rege immer an einen Perspektivwechsel vorzunehmen, um den Sachverhalt nachhaltig erfassen zu können. Machen wir uns also mal Gedanken, was wir selbst machen würden, wenn wir Betrüger wären.

Woher bekomme ich gute Daten?

Also nicht nur vollständige, sondern idealerweise auch welche, von denen auszugehen ist, dass diese eine gute Bonität haben. Schließlich ist es heute absoluter Standard im Kreditgeschäft als Kreditgeber eine Bonitätsprüfung über meinen Kunden durchzuführen. Hierzu sei angemerkt, dass eine Ware, die mit der Bezahlmethode „Kauf auf Rechnung" erworben wird als „auf Kredit gekauft" anzusehen ist Nicht umsonst ist der kriminalistische Begriff dazu „Warenkreditbetrug".

Eine Antwort auf die vorbezeichnete Datenerlangung ist immer die Aussage „im Darknet". Dort bekomme ich grundsätzlich alles: Personaldaten, Kreditkartendaten, Drogen, Waffen, Anleitungen zum Bombenbau und sogar Handgranaten und Panzer. Ich persönlich mag diese Floskel „im Darknet" nicht; und zwar deswegen nicht, weil es so ein „in-die-Ecke-schieben" ist à la „das machen nur Kriminelle, die gut mit dem PC umgehen können – und das sind nur wenige." Also „Cyberkriminelle", ein Begriff unter dem sich viele fehlgeleitete Nerds vorstellen, die 24/7 am Rechner sitzen und Dinge machen, die dem Standard-User wenig verständlich sind. Tatsächlich sind es jedoch vielfach Menschen wie Du und ich – halt nur kriminell.

Es gibt keine Studie darüber, wie die Täter, die im Darknet Personaldaten verkaufen, vorher an diese Daten gelangt sind. Ich persönlich vermute, dass diese im Wesentlichen durch Phishing- beziehungsweise Hacking-Angriffe erlangt wurden. In den letzten Jahren zeichnet sich gefühlt eine gewisse Signifikanz ab, dass insbesondere Daten aus

IDENTITÄTSDIEBSTAHL ALS DIENSTLEISTUNG

Identitätsdiebstähle zählen statistisch betrachtet zu Cyberkriminalität. Meist nehmen sie ihren Ausgang in Ransomware-Angriffen auf Unternehmen, bei denen die Angreifer Millionen von Kundendaten erbeuten, darunter Namen, Anschriften, Geburtsdaten, Handynummern und nicht selten Daten von Personalausweisen und Kreditkarten. Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) gehört Indentitätsdiebstahl neben Ransomware-Angriffen auf Unternehmen und Verwaltungen zu den Top-Bedrohungen durch Cyber-Kriminelle. 84 Prozent aller betrügerischen E-Mails zielten darauf, Authentifizierungsdaten meist von Banken und Sparkassen zu erbeuten, heißt es in dem kürzlich erschienenen BSI-Bericht „Die Lage der IT-Sicherheit in Deutschland 2023", der den Zeitraum zwischen Juni 2022 und Juni 2023 betrachtet. „Phishing-as-a-Service" (PhaaS) nimmt dabei eine Sonderstellung ein. Mittlerweile gibt es laut BSI viele Anbieter, die sozusagen als Dienstleister für Angreifern fungieren und unter anderem Phishing-E-Mails erstellen und versenden, gefälschte Websites und Köderseiten entwickeln und sogar technischen Support und Schritt-für-Schritt-Tutorials anbieten. Gängig sind Phishing-Proxy-Services, die als Man-in-the- Middle (MITM) zwischen Opfer und der Login-Seite eines Unternehmens agieren. Sie können Zugangsdaten und Cookies stehlen und damit beispielsweise eine Multifaktor-Authentifizierungen umgehen. Phishing-Angriffe sind nicht zuletzt durch PhaaS-Dienstleister auch für weniger fortschrittliche Angreifer möglich, wie es in dem Bericht heißt. Mittlerweile sind Angriffe über Social Media, SMS und Voice Calls möglich. „Für Verbraucherinnen und Verbraucher bildet Identitätsdiebstahl und Online-Betrag aktuell die größte Bedrohung", stellt die Studie fest. *chd*

Den vollständigen Bericht können Sie hier nachlesen:

▶ https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=6

Hacking-Angriffen auf die Server von Sportvereinen und Fitneßstudios oft verkauft werden.

Es gibt aber auch andere Quellen, um an gute Daten zu gelangen. Zwei von diesen möchte ich vorstellen, um den anderen Betrüger, den „Nicht-Cyberkriminellen", plastischer darzustellen.

Der verlorene / gestohlene Personalausweis:

Dazu ein Szenario …

Sowohl als zweitgrößte Stadt Deutschlands als auch kulturelle Hochburg im Norden der Republik ist Hamburg quasi ein Magnet für Taschendiebe. Die in Hamburg stattfindenden und jährlich wiederkehrenden Events wie der Schlagermove, der Hafengeburtstag oder die Harley-Days ziehen Zehntausende und auch mal über Hunderttausende an. In den sich drängenden Menschenmassen erzielen Taschendiebe situationsbedingt hohe Erfolge. Aber auch das wöchentliche Geschehen rund um die sündigste Meile der Welt, die Reeperbahn, bietet Taschendieben eine hervorragende Arbeitsgrundlage.

Ziel der Diebe sind vorwiegend Portemonnaies und technische Devices, insbesondere Smartphones und Tablets, die die Taschendiebe an Hehler weiterverkaufen. Seit jeher wurden aber auch die in den Portemonnaies entwendeten Debit- und Kreditkarten teilweise von den Tätern selbst eingesetzt oder aber an Kartenhehler weitergereicht, welche diese mannigfaltig einsetzten. Mit der gestiegenen Zahl sich in Deutschland aufhaltenden illegalen Menschen wurde auch die in den Portemonnaies enthaltenen Krankenkassenkarten immer beliebter. Schließlich werden auch sich illegal aufhaltende Personen krank und müssen mal zum Arzt.

Zu guter Letzt ist zu erkennen, dass mit der Professionalisierung der Betrugsbegehung der Bundespersonalausweis stark ins Visier der Diebe gerückt ist: In Hamburg werden wöchentlich rund 200 Portemonnaies gestohlen. Da es keine Auswertung oder Statistik dazu gibt, kann nur geschätzt werden, wie viele der darin enthaltenden Bundespersonalausweise anschließend für Betrugstaten genutzt werden. Ich persönlich schätze diese Zahl auf ca. 10 bis 20 Prozent.

Zu diesen rund 200 Personalausweisen kommen noch alle weiteren Personalausweise, die verloren wurden. Hierzu gibt es keine Zahl und auch keine Schätzung. Diese verlorenen Ausweise werden teilweise vom ehrlichen Finder abgegeben oder aber vom unehrlichen Finder betrügerisch eingesetzt.

In jedem Fall kann der Betrüger nun mühelos die Personaldaten für seine Betrugsdaten vom Bundespersonalausweis abtippen. Zudem verfügen Betrüger regelhaft über ein gewisses Netzwerk. Befindet sich in diesem Netzwerk nun eine Person, die dem Lichtbild auf dem Personalausweis annähernd ähnlich sieht, stehen dem temporären Duo Tür und Tor offen für zahlreiche Taten mit erheblichen Ertragssummen – 30 bis 40 Waren werden dann durchschnittlich erworben, im Wert von durchschnittlich jeweils 500 Euro.

Um die fünf Mobilfunkverträge werden betrügerisch abgeschlossen und das damit jeweils subventionierte Smartphone erlangt sowie einige Kleinkredite über 5.000 bis 10.000 Euro getätigt. Ab und an gelingt auch mal ein größerer Kredit über 30.000 bis 50.000 Euro. So gesehen ist ein Bundespersonalausweis am Ende gute 50.000 bis 100.000 Euro wert. Davon mal ganz abgesehen, dass es Tätergruppierungen gibt, die damit hochwertige Kfz leasen und/oder finan-

zieren und diese dann zum Ausschlachten oder zur Nutzung ins Ausland verbringen. Das ist aber eine eigene Geschichte wert. Verbleiben wir beim „Normalfall".

Der betrügerische Ertrag mit einem deliktisch verwendeten Bundespersonsalausweis kann zwar eine hohe Summe betragen, ist jedoch wenig skalierbar.... und Skalierbarkeit ist immer ein großer Wunsch eines jeden Unternehmers.

Ja, richtig, „Unternehmer"! Seit Jahren plädiere ich dafür bei diesen professionell angelegten Betrugstaten von einem „Industriezweig" zu reden und in „Business-Cases" zu denken.

Begleitend zu diesem Gedanken werfen wir einen Blick auf die zweite Quelle, wie Täter an „gute" Daten gelangen.

Sie bestellen die Daten per Abo nach Hause!

Ist sogar ganz einfach. Eine bequeme Art und Weise ist „Der öffentliche Anzeiger". In diesem werden handelsregisterliche Neueintragungen veröffentlicht.

Hat also die „XY-GmbH" einen neuen Geschäftsführer oder Prokuristen, wird diese Tatsache im „Öffentlichen Anzeiger" kundgetan. Diese Personen werden dann per Vor- und Nachnamen nebst Geburtsdatum und Wohnort genannt. Für Betrugsdaten im E-Commerce reichen diese Daten völlig aus. Der Täter legt korrespondierend dazu noch schnell eine E-Mail-Adresse an, beispielsweise Vorname.Nachname@t-online.de, sucht noch irgendeine Adresse auf Google-Maps passend zum Wohnort aus und schon kann es losgehen.

Prüft der Onlinehändler nun bei einer Auskunftei seiner Wahl die Daten auf Echtheit, wird er als Antwort immer bekommen: „Ja, Vor- und Nachname mit dem Geburtsdatum kennen wir. Den Wohnort auch. Allerdings die exakte Adresse nicht". Nun kann sich der Händler selbst überlegen, was er machen will. Den Kauf ablehnen oder „denken", dass der Neukunde womöglich umgezogen ist und diese Tatsache der Auskunftei vielleicht noch nicht bekannt ist. Und natürlich freut er sich über Neukunden. Oft genug ist es ein zahlender Neukunde, so dass sich die Annahme von Betrügern als Neukunde noch nicht als zu sehr schmerzend erweist und „ertragen" werden kann.

Werfen wir an dieser Stelle einen kurzen Blick auf den einleitenden Begriff „Identitätsdiebstahl".

Der Diebstahl gemäß § 242 StGB ist ein strafrechtlicher Begriff und meint die „Wegnahme einer fremden beweglichen Sache". Hierunter könnte man den bereits erwähnten Bundespersonalausweis subsumieren. Den bloßen Einsatz der Daten, aber auch der Daten des gestohlenen Bundespersonalausweises vermag ich nicht als „Diebstahl" zu bezeichnen. Vielmehr handelt es sich um eine missbräuchliche oder betrügerische Verwendung. Aus diesem Grund hat sich unter Fachleuten der Begriff des „Identitätsmissbrauches" durchgesetzt. Dieser beschreibt nämlich auch die missbräuchliche Nutzung zum Nachteil des echten Identitätsinhabers. Im Gegensatz dazu ist ein „Identitätsbetrug" bereits dann gegeben, wenn beispielsweise ein jüngerer Bruder den Personalausweis seines älteren Bruders benutzt, um Hochprozentiges oder Zigaretten zu kaufen. Hierbei erleidet der Identitätsinhaber allerdings keinen finanziellen Schaden, es liegt also kein schädlicher „Missbrauch" vor.

Man merkt schnell, dass es doch recht hilfreich wäre, wenn Online-Händler die eingegebenen Daten transparenter prüfen könnten, damit Betrug vermieden werden kann. Hierbei möchte ich den Blick jedoch nicht auf den zu vermeidenden Schaden bei den Unternehmen richten, sondern vielmehr auf die Schäden, die die Personen erleiden, deren Daten missbräuchlich verwendet werden.

WAS BETROFFENE BERICHTEN

DAME-Preisträgerin Sabrina Wolf gewann mit Reportage über Identitätsdiebstahl in Jobportalen

Die Fernseh- und Radiojournalistin Sabrina Wolf beschäftigt sich seit 15 Jahren mit Datenklau und Datenmissbrauch. Für ihre Reportage „Identitätsdiebstahl über Jobportale" recherchierte sie zunächst für die ARD-Sendung „report München", im Anschluss verfasste sie aus dem Material den Radiobeitrag „Vorsicht bei Online-Jobplattformen", mit dem sie sich beim Datenschutz Medienpreis (DAME) des BvD bewarb.

Hier können Sie den Beitrag anhören:

▶ https://www.br.de/radio/br24/sendungen/der-funkstreifzug/datenklau-identitaetsdiebstahl-jobportal-100.html

Dazu werfen wir noch eben einen genaueren Blick auf das Tatgeschehen.

Wie bereits erwähnt, legen Täter zu den erlangten Personaldaten E-Mail-Adressen an und gehen dann online shoppen. Ist dem Täter die Wohnadresse nicht bekannt, sondern nur der Wohnort, lässt er die Ware an eine x-beliebige Adresse des gleichen Wohnortes senden. Kennt er die Adresse (weil ihm zum Beispiel der gestohlene Personalausweis vorliegt), lässt er die Ware zum Opfer nach Hause senden.

In beiden Fällen erhält der Täter über die von ihm angelegte und verwendete E-Mail-Adresse die Benachrichtigung vom Händler, dass dieser die Ware an den Paketzusteller wie DHL oder Hermes übergeben hat. Nun heißt es noch ein bis zwei Tage warten, bis sich der Paketzusteller per Mail meldet und die Zustellung für den Folgetag avisiert.

Nun ändert der Täter bequem die Zustelladresse an eine vorher von ihm ausgespähte und manipulierte Adresse – zum Beispiel durch Überkleben des Briefkastens einer leerstehenden Wohnung oder aber er lässt die Ware an eine Paketstation oder einen Paketshop senden. Zuvor hat der Täter unter Angabe einer Fake-ID ein Kundenkonto für Paketstationen eröffnet oder aber – im Falle der Abholung beim Paketshop – fälscht er kurzerhand eine Vollmacht zur Abholung beim Paketshop.

Idealerweise legt er dazu noch den gestohlenen Bundespersonalausweis vor und begleitet dies mit einer Floskel wie „zum Beweis der Richtigkeit hat mir der XY extra seinen Personalausweis mitgegeben."

Wenn man sich jetzt mal überlegt, wie viele dieser Taten man an einem „normalen" Arbeitstag, also in acht Stunden erledigen kann, dann bekommt der Begriff „skalierbar" doch wohl leider eine handfeste Bedeutung.

Zur Bekämpfung dieser Szenarien gibt es unterschiedliche Ansatzpunkte. Die Betrugsprävention selbst ist mittlerweile auch – wie der Betrug – zu einem Business-Case avanciert und nahezu ein Industriezweig geworden.

So werden unter anderem die IMEI-Daten von Online-Bestellungen von Tablets oder Smartphones ausgewertet, kundenuntypisches Kaufverhalten als „auffällig" ausgesteuert und manuell überprüft und sogar das bloße Tippverhalten bei der Eingabe im Rahmen der Online-Bestellungen wird dahingehend ausgewertet, dass zu langsames Tippen der eigenen Daten als „betrugsauffällig" bewertet wird.

In meinen Augen wäre es wünschenswert, wenn es – auf welcher Basis auch immer – eine „online-Identität" gäbe. Kunden könnten (oder müssten) sich nachhaltig mit all ihren relevanten Daten, insbesondere inklusive E-Mail-Adresse(n) und Mobilfunknummer(n), legitimieren. So könnten dann Online-Händler die eingehenden Daten mit diesem „Pool" abgleichen und erfahren, wenn es „Abweichungen" gibt, die als betrugsverdächtig zu werten wären.

Diese Lösung gut und sicher zu gestaltet halte ich für eine gute und notwendige Möglichkeit den Bürgern die bequeme Bezahlmethode „Kauf auf Rechnung" erhalten zu können, weil so der missbräuchliche Einsatz ausgespähter oder gestohlener Identitäten extrem erschwert wäre.

Dies halte ich deswegen für erstrebenswert, weil Opfer, dessen Daten ausgiebig missbräuchlich genutzt wurden, teilweise erheblich leiden.

In finanzieller Hinsicht werden sie aus dem Nichts mit zahlreichen Rechnungen, Mahnungen und sogar Mahnbescheiden konfrontiert. Ohnmächtig ob dieser Flut wissen viele nicht damit umzugehen und erkennen das Problem nicht richtig.

Oft dauert es Monate, bis die Händler endlich Ruhe geben und verstanden haben, dass der Schuldner selbst Opfer ist. Schließlich könnte es sich auch um eine Ausrede eines Betrügers handeln, der schlichtweg behauptet, seine Daten seien missbräuchlich von einer unbekannten Person genutzt worden. Diese zähe Auseinandersetzung des Opfers mit den Händlern bedeutet einen erheblich Verlust der Lebensqualität. Oft muss das Opfer einen Rechtsanwalt bemühen, der sich der abwehrenden Korrespondenz annimmt.

Dieser Rechtsanwalt ist dann leider natürlich vom Opfer zu zahlen. Kämpft das Opfer nicht schnell und intensiv genug gegen die Mahnflut an, führt dies regelhaft zum Verlust der Bonität und oft auch zum Verlust der Kreditfähigkeit. Diese Betrachtungsweise auf die Opfer kommt mir seit jeher viel zu kurz und sollte deutlich intensiver in den Mittelpunkt der Handlungsnotwendigkeit rücken.

Bundesweit schreiben Online-Händler durchschnittlich circa zwei Prozent ihres Umsatzes wegen Betrugs ab. Davon entfallen circa 2/3 auf Identitätsmissbrauch. Im Jahr 2022 verzeichnete der Online-Handel rund 85 Milliarden Euro Umsatz. Das entspricht 1,7 Milliarden Euro Gesamtschaden und 1,13 Milliarden Euro Schaden im Rahmen von Identitätsmissbrauch.

Also müssen sich Bürgerinnen und Bürger dieses Landes jedes Jahr gegen 1,13 Milliarden Euro betrügerischer entstandener Forderungen wehren – welch ein K(r)ampf!

Hinzu kommen noch die Schäden aus den betrügerischen Mobilfunkverträgen und den Konsumentenkrediten. Hierzu gibt es leider keine belastbaren Zahlen. Insgesamt halte ich diese jedoch für in etwa gleich groß.

Das ist jedoch nur der finanzielle Aspekt. Opfer erleiden teilweise intensive Belastungsstörungen. Insbesondere alleinstehende Frauen leiden unter Störungen, die darin bestehen, dass sie denken, dass der Täter ja wisse, wo sie wohnt und ihr dort auflauern könnte, um zudringlich oder handgreiflich zu werden.

Opfer haben mir gegenüber berichten, dass sie selbst nach über einem Jahr des Tatgeschehens beim Öffnen des eigenen Briefkastens anfingen zu zittern bei dem Gedanken, der Briefkasten könne wieder Mahnbescheide oder ähnliches enthalten. Zu all den geschilderten Tatbegehungen kommen die eingangs erwähnten Bankkonten, die für Geldwäscheaktivitäten genutzt werden. Aber das ist in diesem unserem Land, welches in Europa allgemein als „Paradies für Geldwäsche“ bekannt ist, eine ganz andere und noch viel größere Geschichte; schließlich werden im Bundesgebiet – je nach Schätzung – jährlich 100 bis 200 Milliarden Euro Geld gewaschen.

Über den Autor

Erik Manke
ist seit über 20 Jahren bei der Hamburg Polizei und Fachbereichsvertreter Kriminalpolizei der Gewerkschaft der Polizei. 2017 gründete er das Beratungs-Unternehmen Nodolos, dass sich der Fraud-Prävention verschrieben hat.

▶ http://nodolos.de/

JÜRGEN HARTZ

„WIR BEFINDEN UNS IN EINER ABSOLUTEN UMBRUCHPHASE“

Datenschutzbeauftragte und Aufsichtsbehörden suchen auf der Herbstkonferenz Wege für einen pragmatischen Datenschutz.

Der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Prof. Dr. Tobias O. Keber

„Wir befinden uns in einer absoluten Umbruchphase.“

Mit diesen Worten begrüßte Baden-Württembergs neuer Landesdatenschutzbeauftragte **Prof. Dr. Tobias O. Keber** die rund 300 Fachleute und Datenschutzbeauftragte, die zur siebten BvD-Herbstkonferenz am 18. und 19. Oktober nach München gekommen waren. Keber hat nachgerechnet: 117 Initiativen hat Brüssel gestartet, die den Datenschutz und die Digitalisierung berühren. Sie sollen zwar Rechtsklarheit insbesondere im Zusammenspiel mit der internationalen Datennutzung und der Verwendung von KI bringen. „Man könnte sich aber aus Perspektive der Gesetzgeber fragen, ob weniger manchmal mehr bringt“, sagte Keber.

Denn die Verwirrung, wie die unterschiedlichen Akte mit der DSGVO zusammenspielen, ist bei Unternehmen, Behörden und Datenschutzbeauftragten groß. Der Auslegungsspielraum sorge für Unsicherheiten, sagte Keber, vor allem das Zusammenspiel mit der DSGVO. Dabei müsse es darum gehen Fragezeichen durch Ausrufungszeichen zu ersetzen, unterstrich er in München.

Thomas Spaeing: „Keine theoretischen, vollkommen überzogenen Foderungen.“

Zuvor hatte bereits BvD-Vorstandsvorsitzender Thomas Spaeing in seiner Begrüßung auf die Schwierigkeiten verwiesen, die ein zunehmend komplexer werdender Datenschutz für die Beratung von Unternehmen und Behörden bedeutet. Vor allem kleine und mittlere Betriebe (KMU) seien nicht in der Lage die teils widersprüchlichen Aussagen der einzelnen Rechtsakte zum Datenschutz umzusetzen. Auch verfügten sie nicht über das Knowhow sich in die verschiedenen Verordnungen juristisch sicher einzuarbeiten. Spaeing warnte, die Gesetzgeber in Brüssel und Berlin dürften keine „theoretischen, vollkommen überzogenen Forderungen“ aufstellen.

Ziel der DSGVO sei es gewesen einen risikobasierten Datenschutz zu entwickeln, der von den Verantwortlichen prozessual umgesetzt werden kann. „Wir entfernen uns davon in immer rasanterem Tempo“, sagte er. Als Datenschutzberater falle es ihm zunehmend schwer die Diskrepanz zwischen den Anforderung und dem unternehmerischen Alltag, zwischen dem angestrebten Zweck des Datenschutzes für Betroffene und dem machmal hohen Theoritisierungsgrad zu erklären.


BvD-Vorstandsvorsitzender Thomas Spaeing

Zugleich appellierte er an die Datenschutzbeauftragten: „Wir Datenschützer tun gut daran den Schutzzweck nicht aus den Augen zu verlieren und uns mit weniger Komplexität zufrieden zu geben anstatt diese zu erhöhen." Wenn Unternehmen und Verwaltungen das Gefühl hätten, etwas Sinnvolles und Machbares sei entstanden, „dann haben wir auch den Betroffenen geholfen".

Der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, Michael Will

Michael Will: „Haben wir noch den Überblick?"

Auf die Wirrungen, die die EU-Akte im Zusammenspiel mit der DSGVO bei vielen auslösen, ging auch Michael Will ein. Der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht und diesjährige Gastgeber betonte in seinem Grußwort, Datenschutzbeauftragte und Aufsichtsbehörden müssten sich gleichermaßen weiterentwickeln. Und aktuell müssten sie wie Bergsteiger den nächsten Hügel erklimmen. Um gut voran zu kommen, benötigten sie ein „gutes Fundament", ein Basislager, um sicher loszukommen. „Aber haben wir noch den Überblick? Haben wir noch die Kontrolle?", fragte Will und appelierte an die Datenschutzbeauftragten, vor den neuen Herausforderungen nicht zu resignieren sondern sich fachlich damit auseinanderzusetzen.

Benjamin Brake, Leiter der Abteilung Digital- und Datenpolitik im Bundesministerium für Digitales und Verkehr, sieht eine rechtssichere Auslegung der verschiedenen zusammenwirkenden Daten-Akte als dringlich an. Deshalb tritt er dafür ein die deutsche Datenschutz-Konferenz (DSK) zu stärken und ihr eine eigene Geschäftsstelle zu ermöglichen. „Datenschutz ist kein Hemmnis für die Digitalisierung", sagte Brake. Vielmehr müsse es für Unternehmen eine klare Rechtsgrundlage geben, um beispielsweise „Privacy by Design" umzusetzen.

Unternehmen, die konkurrenzfähig bleiben wollten, müssten auf Daten setzen. „Deshalb wollen wir die Verfügbarkeit und Nutzung von Daten steigern", sagte Brake. Dabei gehe es aber nicht darum mehr Daten zu erfassen. Vielmehr müsse es klare Regeln geben, was im Rahmen des Datenschutzes rechtssicher sei. Als Beispiel nannte er die Frage von Pseudonymisierung und Anonymisierung. Hier brauche es klare Vorgaben, wann welches Verfahren anzuwenden sei.

Judith Gerlach: „Lähmende Unsicherheit"

Die bayerische Staatsministerin für Digitales, Judith Gerlach, sieht bei Unternehmen und in der Verwaltung gar„eine lähmende Unsicherheit" die DSGVO und die schon vorliegenden neuen Rechtsvorgaben aus Brüssel umzusetzen. Viele blieben lieber „beim Alten" und beließen Verfahren und Prozesse so, wie sie schon immer liefen. Dabei müssten gerade Verwaltungen bürgernäher und überhaupt wieder handlungsfähig werden, forderte Gerlach.

Sie unterstrich, Datenschutz sei eine Leitplanke, kein Hindernis. „Wir müssen es schaffen Datenschutz und Datenverarbeitung dauerhaft zu vereinen." Dazu müsse Datenschutz sehr viel anwenderfreundlich werden. Gerade Verwaltungen hätten kaum Kapazitäten,um sich rechtssicher mit Datenschutz zu beschäftigen, und nicht das Geld,um sich Fachleute einzukaufen. Deshalb begrüße sie den Ansatz auf Beratung und konstruktive Lösungen statt auf Sanktionen zu setzen. „Aufklärung und Beratung müssen Hand in Hand gehen", sagte Gerlach.

Die bayerische Staatsministerin für Digitales, Judith Gerlach

Benjamin Brake: „Die Situation ist gelinde gesagt komplex."

Um in Deutschland auf Seiten der Aufsichtsbehörden klarere Rechtsauslegungen datenschutzrechtlicher Sachverhalte zu erreichen, tritt Benjamin Brake, Leiter der Abteilung „Digital- und Datenpolitik" im Bundesministerium für Digitales und Verkehr, für eine Institutionalisierung der Datenschutzkonferenz von Bund und Ländern (DSK) ein. Im Zuge der ge-

Der Leiter der Abteilung "Digital- und Datenpolitik" im Bundesministerium für Digitales und Verkehr, Benjamin Brake

planten Novelle des Bundesdatenschutzgesetzes (BDSG) soll die DSK aus seiner Sicht sogar eine eigene Geschäftsstelle bekommen – eine Forderung, die die Aufsichtsbehörden selbst schon erhoben hatten. Dabei gehe es nicht darum die Aufsicht zu zentralisieren, sondern die Entscheidungen der Aufsichtsbehörden kohärent zu gestalten, sagte Brake und hofft, eine stärkere DSK könne auch den Datenschutz und die Datennutzung stärken. „Die Situation ist gelinde gesagt komplex", sagte Brake mit Blick auf die Pläne von Bundesgesundheitsminister Karl Lauterbach die Nutzung von medizinischen Daten für Forschung und Wirtschaft zu erleichtern. In Finnland habe sich längst ein System etabliert, dass Opt Out ermöglich, aber nur von wenigen Finnen in Anspruch genommen werde. „Warum geht es in Finnland und nicht hier", fragte Brake. Zudem bräuchten Pseudonymisierung und Anonymisierung klare Vorgaben.

Thomas Petri: „Es stehen große Herausforderungen bevor."

Was auf Datenschutzbeauftragten in Kommunen, in Behörden und der Verwaltung zukommt, machte Prof. Dr. Thomas Petri zur Eröffnung des Behördentags am Freitag deutlich, der sich traditionell an die BvD-Herbsttagung anschließt. „Es stehen große Herausforderungen bevor", sagte der Bayerische Landesbeauftragten für den Datenschutz, vor allem durch die weiteren im Rahmen der EU-Digitalstrategie geplanten Vorhaben.

Auch wenn die EU den Wortlaut der DSGVO nicht anfasst, bedeute dies nicht, dass sich beim Datenschutz nichts ändere, sagte Petri. Um Daten im europäischen Binnenmarkt nutzen zu können, zielten die im Rahmen der EU-Digitalstrategie bereits entwickelten und die noch geplanten Rechtsakte darauf bisherige Defizite bei der Nutzung von Daten aufzufangen und einen Ausgleich zwischen Datenschutz und Datennutzung zu schaffen. Die Rechtsakte sorgten für die Schnittstellen.

Bei der Datennutzung sei es eines der zentralen Ziele, „dass die öffentliche Hand ihren Datenschatz öffnet". Die EU arbeitet laut Petri aktuell an Rechtsakten, die es Behörden, Kommunen und Verwaltungen ermöglichen sollen personenbezogene Daten freizugeben. Der Data Governance Act sei für Behörden der bedeutendste Rechtsakt. Er besage, dass die öffentliche Hand die Daten, die schutzwürdig sind, möglichst weitgehend bereitstellen sollen. „So weit es irgendwie möglich ist.»

Praktisch funktionieren soll dies laut Petri über Prozesse, für die die EU aktuell einen Prototyp entwickelt, der sich auf Gesundheitsdaten bezieht. Dieser European Health Data Space (EHDS) befindet sich laut Petri in fortgeschrittenem Stadium des Gesetzgebungsverfahrens und soll noch in dieser Legislatur durch das EU-Parlament gehen. Der EHDS soll im Einklang mit der DSGVO stehen und gleichzeitig die Verarbeitung von Daten ermöglichen. Wenn er steht, könnte das Grundprinzip auch auf andere Bereiche übertragen werden, etwa auf die Mobilität und Daten aus digitalen Auto-Anwendungen.


Der Bayerische Landesbeauftragten für den Datenschutz, Prof. Dr. Thomas Petri

Bislang aber hat der Prototyp einen Haken: Laut Petri hat der erste Entwurf keine Widerspruchsrechte mehr für Betroffene vorgesehen. Was aber geschieht dann beispielsweise mit Daten von seelisch kranken Menschen oder von Personen mit speziellen genetischen Dispositionen? Dies berühre nicht mehr nur den Datenschutz, sondern die Menschenwürde. „Und die ist unantastbar" sagte Petri. Ein solches Verfahren würde aus seiner Sicht nach deutschem Recht nicht funktionieren. Allerdings regten sich Bedenken an der bisherigen Ausgestaltung des EHDS im EU-Parlament und bei einigen EU-Mitgliedsstaaten. „Es zeichnet sich ab, dass die Idee, dass es keine Betroffenenrechte gibt, vom Tisch ist", sagte Petri.

An die kommunalen und behördlichen Datenschutzbeauftragten appellierte er: „Sie müssen darauf achten, dass das alles compliant bleibt." Aus seiner Sorge über die Umsetzung machte er keinen Hehl: „Auf Sie kommt wirklich etwas zu", sagte er zu den rund 300 Teilnehmenden der Konferenz.

Die BvD-Herbstkonferenz und der anschließende Behördentag am Freitag ist eine Gemeinschaftsveranstaltung des BvD mit dem Bayerischen Landesbeauftragten für Datenschutz, Michael Will, dem Bayerischen Landesamt für Datenschutzaufsicht und dem Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Prof. Dr. Tobias O. Keber. In diesem Jahr stand die zweitägige Veranstaltung unter dem Motto „Next Level Privacy: Fit für die Zukunft." Unter anderem diskutierten die Teilnehmenden über Perspektiven von KI (siehe separaten Beitrag), zum internationalen Datentransfer und zum Beschäftigtendatenschutz.

Über den Autor

Jürgen Hartz

ist BvD-Vorstandsmitglied und zuständig für Veranstaltungen.

BVD-HERBSTKONFERENZ 2024

Die nächste BvD-Herbstkonferenz mit Behördentag findet vom **16. Oktober bis 18. Oktober 2024** in Stuttgart statt.

KI-DATENSCHUTZ ALS KÖNIGSDISZIPLIN

Christina Denz

KI und Datenschutz - das ist für Datenschutzbeauftragte und Aufsichtsbehörden aktuell eine Herausforderung. Auf der BvD-Herbstkonferenz und dem anschließenden Behördentag suchten Fachleute Antworten auf die Frage, wie sich beides verbinden lässt. Der Artificial Intelligence Act (AI Act) aus Brüssel, der KI generell behandelt, könne dabei nur ein erster Schritt hin auf dem Weg zu einer datenschutzrechtlichen Regulierung von KI sein, waren sich die Referentinnen und Referenten einig.

Von Datenschutz als Königsdizsiplin im Dekathlon der (Grund-)Rechte sprach **Dr. h.c. Marit Hansen.** KI sei vielfältig - sowohl in der Entwicklung als auch im Einsatz. Ein „One size fits all"-Ansatz funktioniere daher nicht, erklärte die Landesbeauftragte für Datenschutz Schleswig-Holstein in München. KI müsse Datenschutz und Betroffenenrechte garantieren, Informationssicherheit gewährleisten, sie müsse die demokratische Grundordnung einhalten und dürfe nicht für zielgerichtete Beeinflussung missbraucht werden. Außerdem müsse KI das Urheberrecht und Wettbewerbsrecht respektieren und dürfe nicht einzelne gesellschaftliche Gruppen diskriminieren.

Marit Hansen ist Landesbeauftragte für Datenschutz Schleswig-Holstein. Die Informatikerin erhielt 2020 die Ehrendoktorwürde der Universität Karlstadt in Schweden.

Ihr Fazit: „Datenschutz allein garantiert keine rechtskonforme und faire Lösungen für KI." Für Datenschutzbeauftragte vor Ort und in den Aufsichtsbehörden bedeute dies, sich auf weiteren, bislang unberührten Feldern fortzubilden. Sie empfahl deshalb eine Kooperation der Datenschutzbeauftragten mit anderen Zuständigen, Best-Practice-Beispiele zu sammeln und „eine Gestaltung mit Weitblick".

Patrick Grihn, geschäftsführender Gesellschafter der nextindex GmbH & Co. KG

Fragen zur Umsetzung

Patrick Grihn, geschäftsführender Gesellschafter der nextindex GmbH & Co. KG, ließ seine Präsentation von einer KI generieren - musste aber noch händisch nachbessern. In seinem Vortrag „Die KI weiß, was ich letzten Sommer getan habe" ging er ebenfalls auf datenschutzrechtliche Fragen rund um die Anwendung von generativen KI wie ChatGPT und Dall-E vor dem Hintergrund des AI Acts ein. Der AI Act ziele zwar darauf, die Risiken von KI-Systemen zu reduzieren, sagte Grihn. „Es wirft aber auch Fragen bezüglich seiner Umsetzung und Auswirkung auf."

Die Grundlagen der DSGVO gelten laut Grihn auch im AI Act: Der Zweck der Datenverarbeitung müsse klar formuliert sein, ebenso gebe es die Nachweispflicht und auch das in der DSGVO verankerte Verbot einer automatisierten Entscheidungsfindung im Sinne eines Scoring. Ebenfalls müsse die KI Informationspflichten (gem. Art. 13 DSGVO) und Auskunftspflichten (gem. Art. 15 DSGVO) einhalten. Grihn verwies außerdem auf die Entscheidung des Europäische Gerichtshofs (EuGH) im Juni 2022, der den Auskunftsanspruch bei KI-Anwendungen unterstrich und forderte, dass sämtliche Daten aus KI-Trainings benannt und offengelegt werden müssen.

Das muss laut Grihn insbesondere für KI-Anwendungen in der Medizin etwa zur Früherkennung von Krankheiten gelten. Oder für die Daten von autonom fahrenden Autos. Doch Missbrauch mit KI wie LoveGPT und die mit KI entwickelte Schadsoftwares FraudGPT und Darkbert könne das Gesetz nicht ausschließen, unterstrich Grihn.

Hinzu komme bei vielen Unternehmen eine datenschutzrechtliche Bedenkenlosigkeit im Umgang mit KI, beispielsweise bei dem US-Konzern Adobe, der seine Algorithmen mit Nutzerdaten aus der Adobe-Cloud trainiere. Bei Tesla hatten Mitarbeiter laut Grihn Videos von Kameras in Kundenwagen im Internet geteilt. Und selbst versehentlich könnten Daten aus KI-Anwendungen im Netz landen, wie bei Microsofts KI-Team geschehen.

Aus seiner Skepsis gegenüber den gegenwärtigen Fähigkeiten von KI machte **Dr. Kristof Meding**, KI-Beauftragter des LfdI Baden-Württemberg: in seinem Vortrag „Dieser Text wurde von einer KI geschrieben. Doch wie genau?" keinen Hehl. „Für die nächsten Jahre ist KI sehr stark auf das Vorhandene konzentriert", sagte Meding. Bislang täusche KI Kreativität vor, sie sei aber selbst noch nicht kreativ, sondern errechne Ergebnisse auf Basis von vorhandenen Daten, Texten oder Strukturen.

Dass dies mitunter anders aussehe führt Meding auf die Rechnerleistungen zurück, auf die KI-Systeme mittlerweile zurückgreifen könnten. Zudem gebe es eine große Verfügbarkeit von Daten. Diese müssten aber valide sein, damit die KI stimmige Antworten liefern könne. Bei Übersetzungs- und Bildgenerierungsanwendungen sei dies bereits der Fall.

Auch Dr. Stefan Brink, Geschäftsführender Direktor des Instituts für die Digitalisierung wida und früherer Landesdatenschutzbeauftragter von Baden-Württemberg, hält KI aktuell für noch nicht sonderlich ausgereift. „Ist die KI ein intelligentes Wesen oder eine KI, die nur so tut als sei sie ein intelligentes Wesen", fragte er in seinem Vortrag „Datenschutz in Zeiten von KI". Für ungelöste Probleme sei die KI bislang noch wenig hilfreich, bislang simuliere sie lediglich menschliche Intelligenz.

In der Gesellschaft werde sie jedoch oft als künftiger Herrscher über den Menschen oder als Errettung von Umweltkatastrophen oder sozialer Ungleicheit gefeiert.

Dr. Hans Michael Strepp, Amtschef am Bayerisches Staatsministerium für Digitales

Kann KI die Verwaltung revoluzionieren?

Zu jenen, die KI als Hilfsmittel begrüßen gehört **Dr. Hans Michael Strepp**, Amtschef am Bayerisches Staatsministerium für Digitales. In seinem Vortrag zum Abschluss des Behördentags am Freitag betonte er, dass es gerade in der Verwaltung zahlreiche Aufgaben für KI gebe, mit denen sich Kosten einsparen ließen. Zudem könnten KI-Anwendungen den Fachkräftemangel auffangen, der sich auch in der Verwaltung zeige. Der Datenschutz dürfe dabei nicht zur Disposition gestellt werden, „muss aber praktikabel sein", sagte Strepp.

Als Einsatzgebiete von KI nannte er Beschwerdemanagement, Wissensmanagement, kreative Schreibprozesse und repetitive Aufgaben in der Verwaltung und an den Gerichten. „KI hat das Potenzial, die Arbeit der öffentlichen Verwaltung zu revolutionieren", sagte Strepp. Er betonte, KI-Regulierung sei wichtig und richtig. „Nicht alles, was technisch möglich ist, sollte umgesetzt werden." Deutschland müsse aber zugleich ein innovationsfreundliches Umfeld schaffen. Es dürfe in der Verwaltung keine „Totalregulierung" geben. Vielmehr plädierte er dafür, KI-Anwendungen zu testen und dann in einem zweiten Schritt zu schauen, wo die bestehenden Regelungen für die Verwaltung nachgeschärft werden müssten.

Über die Autorin

Christina Denz

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

DR. NIELS LEPPERHOFF

HÄUFIG GESTELLTE FRAGEN ZU TRUSTED DATA PROCESSOR

1 Einleitung

Bei der Entwicklung der Verhaltensregel Trusted Data Processor standen neben einem Wettbewerbsvorteil für selbstverpflichtete Unternehmen auch Erleichterungen und mehr Rechtsicherheit im Vordergrund. In den Gesprächen zeigt sich, dass an verschiedenen Stellen Unsicherheit und Erklärungsbedarf über die Anwendung vom Trusted Data Processor herrschen. Entlang von häufig gestellten Fragen beleuchtet dieser Beitrag den Nutzen und Einsatz vom Trusted Data Processor in Unternehmen.

Die Verhaltensregeln zum Trusted Data Processor können hier kostenfrei heruntergeladen werden.

▶ https://www.verhaltensregel.eu/verhaltensregel/

Wenn Sie Fragen haben, die dieser Beitrag nicht beantwortet, lade ich Sie ein uns anzusprechen.

2 Was unterscheidet Trusted Data Processor von einer Zertifizierung?

Trusted Data Processor ist eine Verhaltensregel gemäß Art. 40 DS-GVO. Eine Verhaltensregel stellt eine Konkretisierung ausgewählter Anforderungen aus der DS-GVO dar. Sie schafft damit Rechtssicherheit in der Anwendung der DS-GVO. Da die Verhaltensregel inhaltlich von einer Datenschutzaufsichtsbehörde genehmigt werden muss, entfaltet die Genehmigung eine Bindewirkung hinsichtlich des behördlichen Handelns.

Eine Zertifizierung nach Art. 42 DS-GVO dient als Nachweis, dass die DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird. Sie dient auch als Compliance-Nachweis nach außen. Die Zertifizierungskriterien bedürfen einer Genehmigung durch eine Datenschutzaufsichtsbehörde. Die Bindewirkung besteht hier für die Prüfkriterien, nicht für eine konkrete Umsetzung der DS-GVO. Eine Aufsichtsbehörde kann im Einzelfall zum Schluss kommen, dass die zertifizierte Umsetzung der DS-GVO widerspricht.

Damit eine Zertifizierung die von der DS-GVO eingeräumte Wirkung entfaltet, muss sie nach Art. 42 DS-GVO genehmigt und von einer nach Art. 43 DS-GVO akkreditierten Zertifizierungsstelle erteilt worden sein. Zertifikate etwa basierend auf einer ISO-Norm erfüllen die Voraussetzungen nicht, das heißt sie entfalten keine vergleichbare Wirkung.

Unternehmen, die sich einer Verhaltensregel unterworfen haben, oder nach Art. 42 DS-GVO zertifiziert sind, profitieren von zahlreichen Erleichterungen, bspw. bei der Dokumentation oder Bußgeldhöhe (Artt. 24, 28 Abs. 1 und 4, 32 Abs. 1, 35 (nur Verhaltensregel), 46 Abs. 2 lit. e, 83 Abs. 2 lit. j DS-GVO).

Um in den Genuss dieser rechtlichen Vorteile zu kommen, müssen sich Unternehmen auf die Einhaltung einer Verhaltensregel förmlich verpflichten. Das bloße Befolgen reicht nicht aus. Bei Trusted Data Processor erfolgt die Selbstverpflichtung gegenüber der DSZ unter verhaltensregel.eu/antrag/.

3 Welche Anforderungen von Trusted Data Processor gehen über die DS-GVO hinaus?

Keine! Eine Verhaltensregel konkretisiert die DS-GVO (Art. 40 Abs. 2 DS-GVO). Sie darf keine zusätzlichen Anforderungen formulieren.

4 Welchen Nutzen haben Auftragsverarbeiter?

- Rechtssicherheit
- Weniger Diskussionen in Vertragsverhandlungen über Regelungen in der AVV
- Geringerer Aufwand bei Auftraggeberkontrollen
- Sichtbare Compliance
- Bewerbbare Compliance

Mit der Einhaltung von Gesetzen darf grundsätzlich nicht geworben werden. Mit einer Selbstverpflichtung auf Trusted Data Processor darf hingegen geworben werden. Datenschutz-Compliance lässt sich mittels Trusted Data Processor somit werblich herausstellen.

5 Wer darf mitmachen?

Trusted Data Processor richtet sich an Auftragsverarbeiter mit einem Leistungsangebot für den deutschen Markt und Sitz in Deutschland. Die Verarbeitung durch den Auftragsverarbeiter muss in Deutschland stattfinden. Wo Unterauftragsverarbeiter sitzen oder verarbeiten, ist unerheblich.

6 Gilt Trusted Data Processor für das ganze Unternehmen?

Nein. Trusted Data Processor bezieht sich auf „Leistungen". Unter „Leistung" wird eine am Markt angebotene Leistung verstanden. Beispielsweise: Hosting einer Entgeltabrechnungssoftware, Wartung einer Software, Datenvernichtung, Telefonie.

Ein Unternehmen kann sich bspw. für die angebotene Leistung Aktenvernichtung selbstverpflichten ohne seine andere angebotene Leistung Dokumenteinlagerung zu berücksichtigen. Wenn ein Auftragsverarbeiter eine Leistung im Portfolio hat, für die Trusted Data Processor nicht umsetzbar ist oder bei der andere Gründe dagegensprechen, kann er trotzdem mit anderen Leistungen teilnehmen.

7 Wie aufwändig ist die Einführung?

Da Trusted Data Processor rechtliche Vorschriften konkretisiert, gibt es keine zusätzliche Anforderung, die über die DS-GVO hinausgeht. Konkretisieren bedeutet jedoch, dass Prozesse und Muster an die durch Trusted Data Processor erfolgte Standardisierung anzupassen sind. Konkret kann folgender Anpassungsbedarf bestehen:

- Angebot ergänzen
- AVV-Regelungen austauschen
- Prozessbeschreibungen prüfen und ggf. anpassen
- Verpflichtung auf Vertraulichkeit bei Abweichungen ggf. neu einholen
- Eigenkontrolle konzipieren und durchführen
- Kontrolle von Unterauftragsverarbeitern konzipieren und durchführen

8 Muss ich alle Altverträge anpassen?

Nicht zwingend. Kunden, deren AVV von den Vorgaben aus Trusted Data Processor abweicht, sind von der Verhaltensregel und ihren Vorteilen wie einem geringeren Kontrollaufwand nicht umfasst.

Insofern kann das Unternehmen frei entscheiden, ob es Kunden eine Vertragsanpassung anbietet oder nicht.

9 Gibt es Besonderheiten bei Unterauftragsverarbeitern in Drittländern?

Trusted Data Processor sieht keine besonderen Regelungen für Unterauftragsverarbeiter in Drittländern vor. Selbstverständlich gelten die bekannten gesetzlichen Anforderungen aus Artt. 45 ff. DS-GVO.

10 Mache ich mich als DSB nicht überflüssig?

Trusted Data Processor kann und will einen DSB nicht ersetzen. Im Gegenteil, für DSB bietet Trusted Data Processor verschiedene Vorteile. DSB können die enthaltenen Musterprozesse frei verwenden. Es bietet sich an, dass die Eigenkontrolle aus Trusted Data Processor durch einen DSB umgesetzt wird.

11 Wie berechnen sich die Kosten bei Unternehmensgruppen?

Die Kosten berechnen sich nach Anzahl der Leistungen, für die die Selbstverpflichtung auf Trusted Data Processor abgegeben wird. Wenn zwei Konzernunternehmen die gleiche Leistung, bspw. Aktenvernichtung, anbieten, wird die Leistung Aktenvernichtung nur einmal gezählt. Somit zahlen die beiden Konzernunternehmen nur einmal und nicht doppelt.

Die Voraussetzung ist, dass alle teilnehmenden Konzernunternehmen von einem Konzernunternehmen gegenüber der DSZ vertreten werden und alle die gleichen Verträge, Angebote und Prozesse nutzen.

Über den Autor

Dr. Niels Lepperhoff
ist Geschäftsführer der DSZ Datenschutz Zertifizierungsgesellschaft mbH.

▶ https://www.verhaltensregel.eu

EFDPO AUF WACHSTUMSKURS

Dachverband gewinnt vier weitere Verbände und lädt zu zahlreichen Events

Der vom BvD mitinitiierte Dachverband European Federation of Data Protection Officers (EFDPO) ist weiter auf Wachstumskurs, sowohl bei der Gewinnung neuer Mitgliedsverbände als auch bei der Menge angebotener Online- und Präsenzveranstaltungen. Neueste Mitglieder sind vier Berufsverbände aus Finnland, Schweden, Norwegen und Dänemark, die sich als Probemitglieder von den Vorteilen des europäischen Netzwerks überzeugen möchten. Mit ihnen zählt die EFDPO nun 18 nationale Mitgliedsverbände, 10 Verbände mehr als zur Gründung 2019.

Nach dem großen Erfolg des Berliner EFDPO-Kongresses im Mai fanden im Oktober das EFDPO-Panel bei einem Kongress in Prag und der englischsprachige EFDPO-Fachkongress zum Thema Gesundheitsdaten in Paris großen Anklang. Aufzeichnungen der Pariser Vorträge und Diskussionsrunden stehen im Nachgang allen Mitgliedern der EFDPO-Mitgliedsverbände online zur Verfügung. BvD-Mitglieder werden in der E-Mail-Mitgliederinformation informiert, sobald die Inhalte verfügbar sind. Die Konzeption des Pariser Kongresses war das erste Projekt der EFDPO-Arbeitsgruppe „Health Data“.

Kostenlose Online-Veranstaltungen für Mitglieder der EFDPO-Verbände (also auch für BvD-Mitglieder) sind ein weiterer Schwerpunkt der Aktivitäten. Sie bieten die Gelegenheit Perspektiven aus anderen europäischen Ländern auf aktuelle Datenschutzthemen kennenzulernen. Sechs kostenlose Termine gab es allein 2023, beispielsweise Workshops zum Angemessenheitsbeschluss und dem Data Privacy Framework im August und zum Thema Whistleblowing im Oktober. *kfh*

Aktuelle Informationen zu den Events und Aktivitäten der EFDPO finden Sie unter:

▶ efdpo.eu

TELEFON-ERSTBERATUNG
0800 – 22 55 283 (0800 – CALLBVD)

Die BvD-Beratungshotline steht BvD-Mitgliedern für eine kostenlose 15-minütige telefonische Erstberatung zu allen Themen rund um den Datenschutz zur Verfügung. Die juristische Ersteinschätzung leisten die Rechtsanwälte der Kanzlei SDS Sander Schöning PartG mbH. BvD-Mitglieder müssen sich mit ihrer Mitgliedsnummer legitimieren.

Die Hotline ist dienstags bis donnerstags jeweils von 10 bis 12 Uhr und von 15 bis 17 Uhr zu erreichen.

DATENSCHUTZTAG HESSEN & RHEINLAND-PFALZ IM JULI 2023

Against all odds: DSB in Behörden und Ämtern suchen nach ihrer Rolle zwischen Datenschutz und Amtsentscheidungen.

Frankfurt/Main (BvD): Wenn der Bürgermeister will, gelten die Argumente von Datenschutzbeauftragten mitunter wenig. Gerade jene, die in Verwaltung und Ämtern digitale Abläufe DSGVO-sicher machen sollen, unterliegen nicht selten dem politischen Willen. Über Chancen und Strategien Datenschutzgesetze in Verwaltungen durchzusetzen und über aktuelle digitale Herausforderungen in Kommunen und Kreisen diskutierten rund 200 behördliche und betriebliche DSB am 5. Juli in Frankfurt am Main.

Der Datenschutztag Hessen & Rheinland-Pfalz ist eine gemeinsame Konferenz des BvD mit den Datenschutzbeauftragten von Hessen und Rheinland-Pfalz, Prof. Dr. Alexander Roßnagel und Prof. Dr. Dieter Kugelmann. Sie bietet den Teilnehmenden Informationen von den Fachleuten der beiden Aufsichtsbehörden – inklusive des bewährten Formats „Die Aufsichtsbehörden beantworten Ihre Fragen" zum Abschluss des Tages.

Auf der zweiten Veranstaltung und im fünften Jahr der DSGVO zeigte sich: Die Aufgaben für DSB in Kreisen und Kommunen sind so vielfältig, wie es deren Aufgaben sind. Wer in einem Landkreis für Datenschutz-Ordnung sorgen soll, muss Abteilungen und Kolleginnen bei der Bauplanung, im Sozialen, bei kommunalen Vorhaben wie Smart Region oder bei der Videoübertragung von kommunalen Veranstaltungen beraten, muss über Dokumentenabholboxen mit Fingerabdruck und über Datenschutz bei Wahlwerbung Bescheid wissen. Dazu braucht es Erfahrung – und Zeit.

Die aber erhalten nur wenige DSB in Behörden und Ämtern. Viele sollen mit einer 10-Prozent-Stelle die Herausforderungen bewältigen. Andere werden von oben ernannt und ohne Erfahrung und Weiterbildung ins kalte Wasser geworfen. Auch darin mag der Grund liegen, warum die Zahl der Datenschutzbeschwerden bei den Aufsichtsbehörden weiter steigt. Allein beim Hessischen Datenschutzbeauftragten gingen bis Anfang Juli 2023 rund 6.800 Beschwerden ein. 1.750 Meldungen konnte die Behörden bis dato abarbeiten. „Wir werden getrieben von Einzelfällen", sagt Alexander Roßnagel. „Aber wir brauchen Lösungen über den Einzelfall hinaus."

Er plädiert dafür „systematisch vorzugehen", präventiv, gestaltend und so zu agieren, dass es erst gar nicht zu Datenschutzverstößen in Verwaltungen kommt. Und das heißt für ihn: Die Verantwortlichen dazu zu bringen Datenschutz zu gewährleisten und beispielsweise Datenschutmanagement-Software zu installieren. Daran sollten die Aufsichtsbehörden und die Datenschutzbeauftragten gemeinsam arbeiten.

Das betrifft auch Datenauskunftsersuchen, eines der Themen auf dem Datenschutztag Hessen & Rheinland-Pfalz. Oder die Frage, welche Daten Behörden für eine Online-Terminvereinbarung von den Bürgerinnen und Bürger überhaupt benötigen. Oder wie sich Datenschutzbeauftragte verhalten können, wenn ein Bürgermeister trotz des Verstoßes gegen die DSGVO Beiträge für Instagram, Facebook oder die Plattform X (ehemals Twitter) freigibt.

Zum Abschluss gab die stellvertretende Datenschutzbeauftragte von Hessen, Lisa-Marie Lange, einen Einblick in die ihrer Erfahrung nach zähen Verhandlungen zwischen den USA und der EU um das Data Privacy Framework. Aber auch sie ist skeptisch, ob die neue Vereinbarung vor dem Europäischen Gerichtshof Bestand haben wird. „Alle Fragen werden wieder vor Gericht landen und sie bleiben weiter schwierig", zeigte sie sich überzeugt. Zwar seien die Behörden an den neuen Beschluss gebunden. „Leider wird es darüber keine Rechtssicherheit geben", schloss sie ihren Vortrag. *chd*

ENDSPURT ZUR DAME 2023

Die Bewerbungsphase für die mittlerweile siebte Ausgabe des Datenschutz Medienpreises (DAME) geht auf die Zielgerade. Ein entscheidendes Auswahlkriterium, um zu den Nominierten zu gehören, ist die Fähigkeit Datenschutzthemen auf eine Weise zu präsentieren, die ansprechend, leicht verständlich und anschaulich ist. Hier ist Kreativität gefragt.

Traditionsgemäß sind die Vorjahressieger Teil der aktuellen Jury, bestehend aus führenden Datenschutzexpert:innen und Medienexpert:innen. Im Jahr 2022 wurde der DAME-Hauptpreis in Höhe von 3.000 Euro an ein achtköpfiges Autoren-Team der „Süddeutschen Zeitung" vergeben für den Beitrag „Was Google über uns weiß". Der Text war eine Gemeinschaftsarbeit von Sabrina Ebitsch, Berit Kruse, Sophie Menner, Sead Mujic, Leonie Rothacker, Marie-Louise Timcke, Dominik Wierl und David Wünschel.

Die Jury wird voraussichtlich im Februar zusammenkommen, um die besten Einreichungen auszuwählen und letztendlich drei herausragende Beiträge zu nominieren. Die Gewinner werden auf der festlichen Preisverleihung im Rahmen der BvD-Verbandstage am 28. Mai 2024 in Berlin bekannt gegeben. *mng*

Bis zum **6. Dezember 2023** können sich Medienschaffende, Autor:innen und Journalist:innen, aber auch Jugendgruppen und Schulklassen noch mit Videos, Audiobeiträgen, Texten, Clips, Webprojekten oder Songs zu einem Thema rund um den Datenschutz bewerben.

LINK-TIPPS

Onlinekommentar.ch

ist die erste gemeinnützige Plattform für Open-Access-Kommentare in der Schweiz.

▶ onlinekommentar.ch/de/search?q=datenschutz

Daten aus den EU-Staaten

data.europa.eu macht Daten aus den EU-Staaten, darunter viele Daten aus der Verwaltung, frei zugänglich.

▶ data.europa.eu/en

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

CHECKLISTEN ZUR DATEN-SCHUTZ-GRUNDVERORDNUNG

IMPLEMENTIEREN • MITIGIEREN • AUDITIEREN

Dr. Peter Katko

Das Buch erschien erstmalig im Jahr 2020. Durch eine Reihe von Urteilen und Leitlinien der Datenschutz-Aufsichtsbehörden haben sich für die Praxis einige Änderungen ergeben, die in der 2. Auflage berücksichtigt werden. Neu hinzugekommen sind Erläuterungen des vom EDSA genehmigten Zertifizierungsstandard „Europrivacy" sowie zum Datentransfer unter den EU-Standardvertragsklauseln als Mitigationsinstrument und den damit verbundenen formellen und inhaltlichen Prüfungsanforderungen für Datenexporteure. Außerdem wurde ein neues Kapitel, § 13 Künstliche Intelligenz und Datenschutz, hinzugefügt – vor allem vor dem Hintergrund der automatisierten Entscheidungen nach Art. 22 DSGVO.

Das Buch ist nun in 13. Kapitel gegliedert:

§ 1	Einleitung
§ 2	Accountability: die Rechenschaftspflicht
§ 3	Der Kernprozess des Datenschutzes – neue Verarbeitungen erfassen, bewerten und überwachen
§ 4	Rechtfertigung und Rechtmäßigkeit der Verarbeitung personenbezogener Daten
§ 5	Die Information der betroffenen Personen
§ 6	Auskunft
§ 7	Sonstige Betroffenenrechte
§ 8	Löschen von Daten
§ 9	Datensicherheit sowie technische und organisatorische Maßnahmen
§ 10	Meldungen und Benachrichtigung von Sicherheitsvorfällen
§ 11	Auftragsverarbeitung und gemeinsame Verantwortlichkeit
§ 12	Drittlandtransfers
§ 13	Künstliche Intelligenz und Datenschutz

Anhang: Zusammengefasste Checklisten

DR. PETER KATKO
CHECKLISTEN ZUR DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

VERLAG C.H. BECK

2. Auflage 2023
268 Seiten
49,00 €
ISBN: 978-3-406-79542-8

Auf der Webseite des Beck-Verlages sind jetzt – was bei der 1. Auflage noch nicht der Fall war – das Inhaltsverzeichnis und das Sachverzeichnis sowie eine Leseprobe abrufbar.

Ebenfalls neu und für die Praxis sehr hilfreich: Im Anhang sind alle Fragen übersichtlich und kapitelweise zusammengefasst.

Das Buch fällt aus dem klassischen Rahmen der Fachliteratur heraus. Der Ansatz wird schon im Titel deutlich. Das Buch ist kein juristischer Kommentar und kein „Erklärbuch". Es arbeitet die Datenschutz-Grundverordnung auch nicht Norm für Norm ab. Es verfolgt einen durchaus praxisorientierten Ansatz, um das Ziel zu erreichen den Datenschutz in die Praxis umzusetzen. Dies geschieht anhand von Fragen. Der Fließtext wird an geeigneten Stellen durch Fragen unterbrochen und die Fragen werden durch Erläuterungen ergänzt. Richtige Maßnahmen werden nicht an die Hand gegeben. Was ist z.B. eine Maßnahme, die der Integrität dient? Auch in der 2. Auflage fehlen Beispiele z.B. als konkrete Einzelmaßnahmen. Dies würde einer „Praxishilfe" (mehr) entsprechen.

Fazit:

In der 2. Auflage sind alle Fragen des Buches kapitelweise im Anhang zusammengefasst. Dies erleichtert und vereinfacht die Arbeit mit dem Werk erheblich. Das Buch hilft Datenschutzbeauftragten bei der Einführung und vor allem durch die Fragen bei der Überprüfung des Datenschutz-Managementsystems. Schön wäre es jetzt noch, wenn der Fragenkatalog, also der neu hinzugekommene Anhang, online verfügbar wäre.

Es ist ein rundum sehr empfehlenswertes Fachbuch geworden, das bei der datenschutzrechtlichen Beratung und Bewertung in der Praxis unterstützt.

RECHT DER INFORMATIONS-SICHERHEIT

BSIG, EU CYBERSECURITY ACT, DS-GVO KOMMENTAR

Kipker/Reusch/Ritter (Hrsg.)

Informationssicherheit, Cybersecurity, IT-Sicherheit und Datensicherheit können nicht im „luftleeren Raum" stattfinden, sondern müssen mit Leitsätzen und konkretisierenden Vorgaben verbunden sein. Dies ist Aufgabe der Gesetzgebung zur Informationssicherheit, der sich dieser Kommentar widmet – natürlich auch mit Blick auf das europäische Recht, denn Cybersecurity kann schließlich nicht an nationalen Grenzen halt machen.

Das Werk ist ein (fast) klassischer Kommentar, Hardcover (Leinen), umfasst 1.032 Seiten und gehört zur Reihe „Gelbe Kommentare" des C.H.Beck Verlages. Neben den drei Herausgebern Prof. Dr. Dennis-Kenji Kipker, Philipp Reusch und Steve Ritter haben 18 sehr renommierte Autoren mitgewirkt.

Es geht um Informationssicherheit, was natürlich auch etwas mit Datenschutz zu tun hat. Der Kommentar enthält auch die Datenschutz-Grundverordnung, allerdings nur drei Normen, denn in Summe geht es um das Thema Informationssicherheit. Abgedruckt und kommentiert sind die Artikel 5, 24 und 32, also die Normen der Datenschutz-Grundverordnung, in denen es um die Sicherheit der Verarbeitung geht.

Darüber hinaus kommentiert das Werk umfangreich u.a. relevante Normen der BSI-KRITIS Verordnung, des Atomgesetzes, des Energiewirtschaftsgesetzes, des Telekommunikationsgesetzes, des Telekommunikations-Telemedien-Datenschutz-Gesetzes und der ENISA. Die ersten 498 Seiten befassen sich intensiv mit dem BSI-Gesetz und der BSI-KRITIS Verordnung.

Das Buch ist kein Praxiskommentar im herkömmlichen Sinne und enthält keine Checklisten und Grafiken. Es ist eine wissenschaftliche Auseinandersetzung und vertiefte Beleuchtung der Probleme rund um die kommentierten Normen. Es ist ein durchaus wissenschaftliches Werk, das sich speziell mit dem Rechtsgebiet der Informationssicherheit befasst. Zielgruppe der Arbeitshilfe ist daher jeder, der im KRITIS Bereich tätig oder beratend tätig ist. Auch wenn es nicht direkt umgesetzt werden muss, gibt der Kommentar viele Denkanstöße und Anregungen, wie man sich einem Thema nähern kann.

Der Kommentar enthält ein sehr ausführliches Stichwortverzeichnis, was die Suche erleichtert. Darüber hinaus enthält er sehr umfangreiche Hinweise auf weiterführende Literatur. Diese Quellen sind in der Praxis als Ausgangspunkt hilfreich, insbesondere wenn man sich in Themen einarbeiten muss. Für diejenigen, die im Bereich KRITIS arbeiten, ist das Buch eine Pflichtlektüre. Für alle anderen ist es auf jeden Fall ein sehr hilfreiches „Nachschlagewerk", wenn man konkret etwas zum Recht der Informationssicherheit sucht.

Der Kommentar ist aktuell und systematisch aufbereitet, verständlich und detailliert formuliert. Er ist derzeit das einzige Werk dieser Art und in dieser Zusammenstellung und stellt das Recht der Informationssicherheit übersichtlich und ausführlich in einem Band dar – ein rundum sehr gelungenes und empfehlenswertes Werk.

Kipker/Reusch/Ritter (Hrsg.)
RECHT DER INFORMATIONSSICHERHEIT

C.H.BECK

1. Auflage 2023
1.032 Seiten
139,00 €
ISBN: 978-3-406-78339-5

Rezensionen von

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

▶ AdOrgaSolutions.de

KÜNSTLICHE INTELLIGENZ IM ÖFFENTLICHEN SEKTOR

VERFASSUNGS- UND DATENSCHUTZRECHTLICHER RAHMEN FÜR DEN STAATLICHEN EINSATZ INTELLIGENTER TECHNOLOGIEN

Behrang Raji

Behrang Raji behandelt in seiner im Duncker & Humblot Verlag erschienenen Dissertationsschrift ein hochgradig aktuelles Thema. Die Künstliche Intelligenz („KI“) hält Einzug in die öffentliche Verwaltung bzw. soll neue Impulse für die Entbürokratisierung deutscher Behörden schaffen.

Zum Autor

Behrang Raji war bis November 2022 als Referent beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit beschäftigt. In dessen Amtszeit fiel insbesondere auch das Gesetzgebungsverfahren zur polizeirechtlichen „Data-Mining“ Vorschrift des § 49 des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei Hamburg, die vom Bundesverfassungsgericht in seiner Entscheidung vom 16.02.2023 für verfassungswidrig erklärt worden ist. Diese Rahmenbedingungen lassen erwarten, dass die Arbeit gleichermaßen Impulse für die Rechtswissenschaft sowie die Verwaltungspraxis in den Behörden enthält.

Technik und Einsatzbereiche von KI-Systemen

Der Lebensbereich von KI-Systemen im öffentlichen Sektor wird auf rund 119 Seiten der 254-seitigen Dissertation dargestellt. Nach einer Einleitung (S. 23–40) beschreibt Herr Raji die Technologie, die sich hinter dem Schlagwort Künstliche Intelligenz verbirgt (S. 42–84). Ein KI-System sei ein Entscheidungssystem, das in mindestens zwei Prozessschritten entwickelt werden müsse (S. 65). Der erste Algorithmus würde auf Basis von Daten ein statistisches Modell entwickeln; der zweite Algorithmus würde auf Basis des statistischen Modells nach einer Dateneingabe eine neue Entscheidung generieren (ebd.). Sodann werden Stärke und Schwächen verschiedener Lernmodelle erläutert. Die Ausführungen sind eingängig und auch für technische Laien nachvollziehbar.

Im zweiten Teil dieses Abschnitts werden exemplarisch einige Einsatzfelder von KI-Systemen im Bereich des Strafrechts und des Gefahrenabwehrrechts beschrieben. Das amerikanische System COMPAS, das Richtern im Zusammenhang mit Strafaussetzung, Untersuchungshaft und Festlegung der Haftlänge Hilfestellungen gibt, wird kritisch analysiert (S. 86 ff.). Das Beispiel ist treffend gewählt, zeigt es doch die Grenzen der aktuellen Technik auf, die keine Kausalitäten, sondern Korrelationen erzeugt. KI-Systeme werden mit Daten aus der Vergangenheit angelernt und teilen diese Daten in Gruppen ein. Dies würde mit dem Schuldprinzip des deutschen Strafrechts, das gerade an die individuelle Schuld eines Täters oder eine Täterin anknüpft, in einem Spannungsverhältnis stehen. Man könnte nun argumentieren, dass das KI-System doch lediglich assistiert eingesetzt wird und immer ein menschlicher Richter die Entscheidung überstimmen kann. Nun, so einfach ist es nach Ansicht von Herrn Raji wohl nicht: Im Rahmen einer Studie sollten 52 deutsche Richter, bevor sie über das Strafmaß eines fiktiven Angeklagten entscheiden, einen Würfel werfen. Die Richter, die eine hohe Zahl geworfen hatten, neigten dazu, im Vergleich mit solchen Richtern, die eine niedrige Zahl erwürfelt hatten, eine höhere Haftstrafe zu verhängen (S. 58).

Behrang Raji
KÜNSTLICHE INTELLIGENZ IM ÖFFENTLICHEN SEKTOR

DUNCKER & HOMBLOT

1. Auflage 2023
273 Seiten
79,90 €
ISBN: 978-3-428-18838-3

Die bloße Kenntnisnahme von einer Zahl hatte daher Einfluss auf die Entscheidung der Richter. Mit diesem Beispiel beschreibt Raji den sog. „Ankereffekt". Dieser Effekt tritt auf, wenn Menschen einen bestimmten Wert, etwa eine Zahl, für eine unbekannte Größe erwägen, bevor sie diese Größe „für sich" abgeschätzt haben (S.57). Der im Vorfeld angegebene Wert würde wie ein „Anker" wirken; er legt den Ausganspunkt der weiteren Überlegungen des Richters fest. Wenn nun das KI-System COMPAS eine bestimmte Zahl, nämlich einen Scorewert, generiert, um die Rückfallwahrscheinlichkeit eines Straftäters abzuschätzen, dann habe der Richter – wenn man den Ergebnissen der Studie folgt – die Tendenz diesen Wert als Anker seiner weiteren Überlegungen zugrunde zu legen. Man kann daher durchaus hinterfragen, ob es überhaupt einen Unterschied macht, ob ein KI-System vollautomatisiert (ohne menschliche Kontrollinstanz) oder assistiert (mit menschlicher Kontrollinstanz) eingesetzt wird (vgl. hierzu auch die Schlussanträge des EuGH-Generalanwalt Pikamae v. 16.03.2023, Az. C-634/21 – SCHUFA-Scoring-Verfahren).

Regulatorische Anknüpfungspunkte beim Einsatz von KI-Systemen

Herr Raji verfolgt mit seiner Dissertation das Ziel den verfassungsrechtlichen Rahmen aufzuzeigen, an dem der Einsatz von KI-Systemen zu messen ist, sowie Regelungslücken zu ermitteln. Dabei lässt Herr Raji die europäische KI-Verordnung außer Betracht, die im Zeitpunkt der Veröffentlichung des Buches erst im Entwurfsstadium vorlag. Diese Reduktion von Komplexität ist aber keine Schwäche des Buches, sondern gerade seine Stärke.

Der verfassungsrechtliche Gleichheitssatz und das Datenschutzrecht bilden eine herausgehobene Rolle für die Bewältigung der Herausforderungen, die mit dem Einsatz von KI-Systemen in der öffentlichen Verwaltung einhergehen. Staatliche Entscheidungen, die auf den errechneten Ergebnissen von KI-Systeme beruhen, die technologiebedingt eine diskriminierende Programmstruktur haben, dürften nicht gegen den verfassungsrechtlichen Gleichheitssatz verstoßen (S.177 u. S. 184).

Es würde aber ein Spannungsfeld zwischen der Genauigkeit der KI-Systeme, die auf eine maximale Zahl an Variablen und Trainingsdaten angewiesen sind, und dem Diskriminierungsverbot der analogen Welt bestehen (ebd.). Das Problem ist, dass KI-Systeme, auch wenn ihnen „verboten wird" ein bestimmtes diskriminierendes Merkmal (z. B. die Hautfarbe) zu verarbeiten, trotzdem zu diskriminierenden Ergebnissen kommen. Die KI-Systeme würden in den Daten inhärente soziale Muster ermitteln, sodass z. B. durch die Berücksichtigung des Einkommens dunkelhäutige Menschen trotzdem in einer bestimmten Gruppe zusammengefasst werden würden. In der Konsequenz dürften daher die Variablen, die in der analogen Welt dem Minderheitenschutz dienen, gerade nicht einer Verarbeitung durch das KI-System vorenthalten werden (S. 184). Dieses Ergebnis mag auf den ersten Zugriff kontraintuitiv sein, aber je weniger Daten ein KI-System über Minderheiten hat, desto ungenauer sind die Aussagen des KI-Systems über Minderheiten. Ob das Datenschutzschutzrecht als präventiver Vorfeldschutz allein in der Lage ist diese Risiken zu bewältigen, wird an dieser Stelle nicht verraten (hierzu: S. 187 ff.).

Die Dissertationsschrift von Herr Raji sei allen Lesern empfohlen, die im öffentlichen Datenschutzrecht beraten und für die das öffentliche Datenschutzrecht eine wesentliche Rolle bei der Ausführung staatlicher Aufgaben spielt, weil sie wichtige Impulse für die zukünftige Verwaltungspraxis enthält.

Rezensionen von

Dr. Dominic Habel
ist Referent beim Landesbeauftragten für den Datenschutz Niedersachsen. Zu seinen Schwerpunkten gehörden die Themen Datenschutzrecht und Medienrecht.

CLOUD COMPUTING NACH DER DATENSCHUTZ-GRUND-VERORDNUNG

AMAZON WEB SERVICES, GOOGLE, MICROSOFT & CLOUDS ANDERER ANBIETER IN DER PRAXIS

Thorsten Hennrich

Das Handbuch bietet eine sehr empfehlenswerte Orientierungshilfe für alle Datenschutzberater und -beauftragten, die sich vielfältig mit dem Thema Cloud Computing in ihrer Praxis auseinandersetzen. Besonders gut hat mir gleich zu Beginn das Kapitel zur Begriffsbestimmung gefallen. Mit großem Erfahrungsschatz berichtet der Autor von immer wieder in der Praxis aufkommendem Meinungsverschiedenheiten zum Cloud-Begriff, den er aus verschiedenen Blickwinkeln beleuchtet und erklärt. Insofern dürfen alle, die die verschiedenen Cloud-Service-Modelle (SaaS, PaaS, IaaS) als unverdaulichen Buchstabensalat für ungenießbar erachten und private, public, hybrid, multi, und community Cloud-Bereitstellungsmodelle als Fachchinesisch verteufeln, mit dem Handbuch Hilfe erwarten. Das Buch bietet daneben eine prägnante und – auch für Datenschutzberater ohne IT-Ausbildung – verständliche Erklärungshilfe inklusive einer sehr nützlichen Darstellung der Vor- und Nachteile der verschiedenen Cloud-Service-Modelle.

Darüber hinaus veranschaulicht das Handbuch die technischen Grundlagen des Cloud Computings in einem für Datenschutzberater und -beauftragte ohne technischen Hintergrund perfekt dosierten Maße. Logik, Zusammenhänge und relevante Basistechnologien (inklusive Virtualisierung, Container-Technologie und Orchestrierungsanwendungen wie z.B. Kubernetes) werden sehr gut erklärt.

Ferner werden die sog. Hyberscaler der Cloud-Industrie (Amazon Web Services, Microsoft und Google) portraitiert. Diebzgl. sei allerdings Vorsicht geboten. Denn die Angebote und ihr Inhalt entpuppen sich in der Praxis als äußerste dynamisch. Insbesondere Details zur Datenlokalisierung sollten ohne individuelle Prüfung ganz generell nicht unreflektiert übernommen werden, weil erfahrungsgemäß der Teufel im Detail steckt.

Besonders positiv sticht indes die Behandlung und schematische Abarbeitung der relevanten Facetten einer äußerst fachkundigen Datenschutzprüfung heraus. So handelt der Autor lehrbuchhaft alle in Rahmen der Datenschutzprüfung relevanten Themen ab. Beginnend mit dem Anwendungsbereich über die Rechtmäßigkeit der Datenverarbeitung, Herausforderungen der Auftragsverarbeitung, die Erstellung von Verarbeitungsverzeichnissen, die Durchführung von Datenschutz-Folgenabschätzungen, Besonderheiten der gemeinsamen Verantwortlichkeit, Datensicherheit (inklusive relevanter Cloud-Zertifizierungen wie z.B. BSI C5), Kontrollen bei grenzüberschreitenden Datentransfers (inklusive der rechtlichen Herausforderungen von Datenzugriffen durch drittstaatliche Stellen unter dem Stichwort „Cloud Act") bis hin zur Behandlung der Geltendmachung von Betroffenenrechten und Datenschutzverletzungen wird alles abgehandelt.

Zum guten Schluss gibt der Autor schließlich noch fachkundige Anleitung für die Auslagerung von Diensten in die Cloud zu in der Praxis äußerst relevanten Besonderheiten regulierter Industrien (z.B. Finanzindustrie) und Bereichen (z.B. öffentlicher Sektor). Abgerundet wird das Werk durch Handlungsempfehlungen zur Bewertung von Angeboten inklusive Kriterien für die Auswahl von Angeboten und die Durchführung von Vertragsverhandlungen.

Alles in allem lautet mein Fazit: Sehr lesenswert.

THORSTEN HENNRICH
CLOUD COMPUTING NACH DER DATENSCHUTZ-GRUNDVERORDNUNG

O'REILLY VERLAG, HEIDELBERG

1. Auflage 2022
342 Seiten
44,90 €
ISBN: 978-3-96009-113-4

Rezension von

Dr. Christoph Bausewein, CIPP/E, CIPT
ist BvD-Vorstandsmitglied und Director & Counsel, Data Protection & Policy bei CrowdStrike.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Heiko Roth

Bei Diskussionen um Entbürokratisierung wird es oft genannt: Das „Verzeichnis der Verarbeitungstätigkeiten" nach Art. 30 DS-GVO. Hier widmet sich nun ein Fachbuch über 300 Seiten diesem Thema. Heiko Roth hat ein Praxisbuch vorgelegt, dass vor allem für Verantwortliche zur praktischen Umsetzung aus rechtlicher, organisatorischer und technischer Sicht gedacht ist. Dieses Ziel hat er gleich als Untertitel gewählt.

Schon im Einstieg führt er aus, wie bedeutsam für ein Management die Kenntnis der einzelnen Prozesse innerhalb der jeweiligen Organisationsstruktur ist, insbesondere, wenn es um die Verarbeitung personenbezogener Daten geht.

Für die Struktur des Modells wird auf die Themenbereiche, Recht, Organisation und IT zurückgegriffen. Das Verzeichnis von Verarbeitungstätigkeiten bietet sich als Prüfungsgegenstand durch Aufsichtsbehörden an, weil dessen Vorliegen und Vollständigkeit anhand der gesetzlichen Anforderungen im Abgleich mit der realen Umsetzung durch Verantwortliche und Auftragsverarbeiter leicht überprüfbar ist. So listet der Autor bereits im 2. Kapitel Umfragen und Einzelprüfungen der Aufsichtsbehörden auch aus anderen Mitgliedsstaaten der EU zum Verzeichnis der Verarbeitungstätigkeiten auf.

Besondere Aufmerksamkeit legt Roth im 3. Kapitel auf Begrifflichkeiten wie „Verarbeitung", „Verarbeitungstätigkeiten" und deren Verhältnis zu „Geschäftsprozessen". Daraus leitet sich die Komplexität eines Verzeichnisses der Verarbeitungstätigkeiten ab, je nachdem wie granular einzelne Schritte zu dokumentieren sind. Hierzu analysiert das Werk unterschiedliche Fundstellen seitens der (europäischen) Aufsichtsbehörden und Kommentarliteratur und stellt diese umfassend dar.

Seinen Wert gewinnt das Werk durch eine gesamtheitliche Betrachtung: Neben der DS-GVO analysiert es auch die Anforderungen aus der Richtlinien „Polizei und Justiz" (EU 2018/680) sowie der Verordnung über die Verarbeitung personenbezogener Daten durch Einrichtungen der EU (EU 2018/1725). Dabei wird die immense Arbeit des Autors deutlich: Auf europäischer Ebene sind deren Einrichtungen zur Veröffentlichung der Verzeichnisse in einem zentralen Register verpflichtet. Der Autor listet die entsprechenden Fundstellen in den Fußnoten auf. Darüber lassen sich für Einsteiger in die Materie wertvolle Erkenntnisse ableiten. Hervorzuheben ist auch die Aktualität der Darstellung, was sich beispielsweise mit der Berücksichtigung der Rechtsprechung des EuGH und seinen Aussagen zu den Konsequenzen bei Verletzungen von Dokumentationsanforderungen 2023 (C-300/21 und C-60/21) zeigt.

Bei vielen Fragestellungen wird die Praxisnähe des Autors zur Thematik deutlich, etwa, wenn er verschiedene Anforderungen europäischer Aufsichtsbehörden zitiert zur Frage, in welcher Sprache das Verzeichnis bei internationalen Konzernen zu führen ist. Oder wen er Hinweise zu einer einheitlichen Taxonomie und zur Enterprise Management Architecture gibt.

Zusammen mit den vielen Abbildungen, Diagrammen und Tabellen, die anschaulich die jeweiligen Thematiken vermitteln, überzeugt dieses Praxishandbuch mit seiner Detailtiefe, den umfassenden Quellenangaben und praxisrelevanten Zusammenfassungen. Nicht nur für Anforderungen im Konzernumfeld, sondern auch für verantwortliche Funktionsträger, die das Verzeichnis der Verarbeitungstätigkeiten als zentrales Hilfsmittel für Managementanforderungen nutzen wollen, ist es uneingeschränkt empfehlenswert. Datenschutzbeauftragte hilft das Werk, diese dabei zu unterstützen.

Heiko Roth
VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

VERLAG: DFV MEDIENGRUPPE

1. Auflage 2023
303 Seiten
Preis 89,00 Euro
ISBN 978-3-8005-1875-3

Rezension von

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

ÜBERBLICK

REZENSIONEN 2023

Titel	Autor	Verlag	Jahr	Erschienen in
KÜNSTLICHE INTELLIGENZ UND ALGORITHMEN IN DER RECHTSANWENDUNG	Prof. Dr. Martin Kment, Sophie Borchert	C.H. Beck	2022	BvD-News 01/2023
DER VORBEHALT MENSCHLICHER ENTSCHEIDUNGEN IM ARBEITSVERHÄLTNIS	Maurice Heine	Verlag Duncker & Humblot	2023	BvD-News 01/2023
DATENSCHUTZRECHT	Prof. Dr. Heinrich Amadeus Wolff, Dr. Stefan Brink (Hrsg.)	C.H. Beck	2022	BvD-News 01/2023
EIN ALGORITHMUS HAT KEIN TAKTGEFÜHL	Katharina Zweig	Heyne	2019	BvD-News 02/2023
DIE DIGITALE TRANSFORMATION DES QUALITÄTSMANAGEMENTS	Gernot Freisinger, Oliver Jöbstl, Bernd Kögler, Jürgen Lipp, Manfred Strohrmann	Carl Hanser Verlag GmbH & Co. KG	2022	BvD-News 02/2023
ENTZAUBERUNG DES RECHTS AUF INFORMATIONELLE SELBSTBESTIMMUNG	Svenja Behrendt	Mohr Siebeck	2023	BvD-News 02/2023
CHECKLISTEN ZUR DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)	Dr. Peter Katko	C.H. Beck	2023	BvD-News 03/2023
RECHT DER INFORMATIONSSICHERHEIT	Kipker/Reusch/Ritter (Hrsg.)	C.H. Beck	2023	BvD-News 03/2023
KÜNSTLICHE INTELLIGENZ IM ÖFFENTLICHEN SEKTOR	Behrang Raji	Duncker & Homblot	2023	BvD-News 03/2023
CLOUD-COMPUTING NACH DER DATENSCHUTZ-GRUNDVERORDUNG	Thorsten Hennrich	O'Reilly	2022	BvD-News 03/2023
VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN	Heiko Roth	Verlag: dfv Mediengruppe	2023	BvD-News 03/2023

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:

04.12.2023	RG Schwäbisch Gmünd
08.12.2023	RG Karlsruhe
18.01.2024	RG Mitte
21.03.2024	RG Mitte
22.03.2024	RG Karlsruhe

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

Termine und Anmeldung finden Sie auf unserer Webseite:

- bvdnet.de/termine/

BVD-STELLENBÖRSE

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

- bvdnet.de/bvd-stellenboerse

VERNETZEN SIE SICH MIT UNS:

- bvdnet.de

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

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

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

RSS-Feed: bvdnet.de/feed/

BVD PARTNERSHIP PROGRAM

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

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

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

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

Karsten Füllhaase
Geschäftsführer
Tel. +49 (0)30 20 62 14 41
▶ karsten.fuellhaase@bvdnet.de

Wir danken unseren Silver Partnern:

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.

BvD-Termine

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Seminare/Webinare:

Termin	Thema
05.12.2023	Online-Seminar: Datenschutzaudit und Datenschutzkontrolle
06.12.2023	Präsenz-Seminar: Umsetzung der internen Meldestelle – mit Workshop-Charakter
07.12.2023	Online-Seminar: Datenschutzverträge in der Unternehmenspraxis
13.12.2023	Online-Seminar: Jura für Datenschutzbeauftragte – Rechtstexte verstehen
23.01.2024	Online-Seminar: KI für kleine und mittlere Unternehmen
20.02.2024	Webinar – Aufbau einer Human Firewall als Sicherheitskonzept gegen Cyberangriffe
21.02.2024	Webinar – Backup, Cloud und Sicherheitskonzepte, was ist der richtige Weg?

BvD-Veranstaltungen:

Termin	Thema
28. – 29.05.2024	BvD-Verbandstage 2024 in Berlin
25.06.2024	3. Datenschutztag Hessen & Rheinland-Pfalz in Frankfurt/Main
16. – 18.10.2024	BvD-Herbstkonferenz & Behördentag in Stuttgart

JETZT ANMELDEN:
bvdnet.de/termine

ÜBERBLICK

DIE THEMEN 2023

IM FOKUS

Rubrik/Thema	Im Fokus/Urteile	Autor:in	Heft-Nr.	Seite
Gesetzlich Grundlage zur automatisierten Daten-Analyse teilweise verfassungswidrig.	Rechtsprechung BVerfG	Maria Christina Rost, Ines Walburg	1/2023	6
Wenn Autos ohne Daten nicht mehr rollen	Mobilität	Marion Jungbluth	1/2023	10
Was das geplante Hinweisgeberschutzgesetz leisten muss	Rechtsprechung BVerfG	Lea Vietze, Vincent Stöber	1/2023	12
Eine neue Epoche?	BvD-Verbandstage 2023	Christina Denz, Jürgen Hartz	2/2023	6
Kennzeichnungspflichten für KI aus Perspektive der Ethik	KI	Jessica Heesen	2/2023	10
Digitalisierung im Gesundheitswesen	Medizin und Datenschutz	Bernd Schütze, Prof. Dr. Klaus Pommerening	2/2023	14
„Wir müssen in eine Art Durchsetzungskultur switchen."	Interview mit Max Schrems	Interview	2/2023	18
„Ganz perfekt ist sie noch nicht" Positionspapier des BvD zur DSGVO-Evaluation 2024.	Veranstaltung zur DSGVO-Evaluation 2024	Christina Denz	3/2023	6
„Eine Pseudonymisierung ist eine faule Ausrede"	Interview mit Carl Fabian Lüpke	Interview	3/2023	14
Neues zu den EU-Datenakten	EU Acts/DSGVO	Kristina Schreiber	3/2023	16

DATENSCHUTZRECHT

Der Zugang von E-Mails im Rahmen der Geltendmachung von Betroffenenrechten	E-Mail und Zustellung	Nicole Schmidt, Lilly Steinbrecher, LL.B., Laura Toska Genkinger	1/2023	16
Das neue Fernmeldegeheimnis	E-Mail und dienstliche Postfächer	Stefan Sander, LL.M., B.Sc.	1/2023	20

DATENSCHUTZRECHT

Rubrik/Thema	Im Fokus/Urteile	Autor:in	Heft-Nr.	Seite
Datenschutzrechtliche Verkehrssicherungspflicht – ein Novum?	DSGVO	Dr. Jens Eckhardt, Dr. h. c. Marit Hansen	2/2023	20
Was Datenschützer über das Strafrecht wissen müssen	DSGVO und StPO	Dr. Eren Basar	2/2023	28
Bestandsdatenauskunft nach dem TTDSG	TTDSG	Matthias Lachenmann	2/2023	32
Europäischer Datenschutz vs. Chinesische Sicherheitsgesetze	Data Transfer Impact Assesment	Dr. Florian Eisenmenger	3/2023	20
Zum aktuellen Stand des Beschäftigtendatenschutzgesetzes	Beschäftigtendatenschutz	Carmen Wegge	3/2023	28

DATENSCHUTZPRAXIS

Microsoft 365:	DSK und Rechenschaftspflicht	Kristin Benedikt	1/2023	28
Lotse durch den Datenschutzdschungel: Der Datenschutzbeauftragte	Compliance und DSGVO	Andrea Backer-Heuveldop, Bernd Schütze	1/2023	32
Den Auftragsverarbeitungsvertrag ausgestalten	DSGVO und Pflichten der Verantwortlichen	Harald Trettow	1/2023	39
„Trusted Data Processor" (TDP) – Regelungsinhalte und Vorteile der Verwendung	Trusted Data Processor	Stephan Rehfeld	1/2023	46
Datenverarbeitung in einem Drittland	Data Transfer Impact Assessment	Regina Mühlich, Bernd Schütze	2/2023	36
Schritt für Schritt zum Datenschutz	Datenschutz für Kleinunternehmen	Carsten Laumann, Kirstin Vedder	2/2023	40
Intersections between the Data Act and GDPR	EU Acts und DSGVO	Petra Miloschewitschova, Jiri Mnuk, Michal Nuliçek	2/2023	44

Rubrik/Thema	Im Fokus/Urteile	Autor:in	Heft-Nr.	Seite
Auftragsverarbeitung nach Art. 28 Abs. 3 lit. g DS-GVO	DSGVO	Haral Trettow	3/2023	24
Standard-Datenschutzmodell 3.0	DSK	Martin Rost	3/2023	28
NIS-2 und Dora: Die EU-Initiativen zur Datensicherheit	Datensicherheit	Thomas Kahl	3/2023	30
AUFSICHTSBEHÖRDEN				
„Wir sehen nach wie vor einen großen Beratungsbedarf."	Interview mit der Datenschutzbeauftragten von Berlin, Meike Kamp	Christina Denz	1/2023	48
KI und Datenschutz	Datenschutzbeauftragter Baden-Württemberg	Dr. Jan Wacke, Dr. Peter Nägele	2/2023	48
Portale, Register, Plattformen	Datenschutzbeauftragte Brandenburg zu internationalem Symposium	Sven Müller	3/2023	34a
Was müssen Unternehmen wissen, wenn Aufsichtsbehörden Auskunft von ihnen verlangen	Hessischer Datenschutzbeauftragter	Maria Christina Rost	3/2023	38
GESELLSCHAFT				
Umgang von Anwenderunternehmen mit dem Datenschutz	IT-Innovationen und Datenschutz	Michael Rath, Dennis Göbel	1/2023	50
Rotkäppchen und das Datenschutzproblem	Pixi-Bücher zum Datenschutz	Christina Denz	2/2023	52
Identitätsdiebstahl und Identitätsmissbrauch	Kriminalität und Prävention	Erik Manke	3/2023	42

AUS DEM VERBAND

Rubrik/Thema	Im Fokus/Urteile	Autor:in	Heft-Nr.	Seite
Von Identitätsdiebstahl, Zeitraub und Datensammelwut	Datenschutz Medienpreis DAME 2022	Christina Denz	1/2023	56
Austausch, Vernetzung, Sichtbarkeit	EFDPO	Karsten Füllhaase	2/2023	54
Spannend und aufklärend: Jury vergibt die DAME 2022	Datenschutz-Medienpreis DAME 2022	Christina Denz	2/2023	58
„Wir befinden uns in einer absoluten Umbruchphase“	BvD-Herbstkonferenz 2023	Jürgen Hartz	3/2023	48
Kurz gefasst • Neue Praktikumsbörse des BvD • Link-Tipp	BvD-Service	diverse	1/2023	58
Kurz gefasst • Vorstand im Amt bestätigt • “Trusted Data Processor” im Überblick • BvD-Beratungshotline für Mitglieder gestartet • Link-Tipp	BvD-Service	diverse	2/2023	62/63
Kurz gefasst • Datenschutz Medienpreis • Datenschutztag Hessen & Rheinland-Pfalz im Juli 2023 • EFDPO auf Wachstumskurs • Telefon-Erstberatung • Link-Tipp	BvD-Service	diverse	3/2023	56 - 58

Schnell & effektiv • Modern & zuverlässig • Zeitsparende Echtzeitlösung

DSGVO-GUARD®

DSGVO-konform im Handumdrehen!

Erleben Sie das absolute Highlight im Datenschutz mit dem DSGVO-Guard®

Wie der DSGVO-Guard® Sie im Alltag unterstützt

- Steigen Sie in die Zukunft des modernen Audits ein und entdecken Sie die **Innovation und Transparenz** des DSGVO-Guard®.
- Dieses webbasierte Tool macht Ihren Alltag mühelos und ermöglicht **schnelle Reaktionen auf Datenschutzanforderungen**.
- Komplette **Rechtstexte in Echtzeit** erhalten (weniger als 9 Minuten) statt stundenlanger manueller Tätigkeit.
- Profitieren Sie von erweiterbaren **White-Label-Rechtstexten**, einer wirtschaftlichen Lösung und **phänomenaler Zeitersparnis**.
- DSGVO-Guard® **analysiert in Echtzeit** alle eingebundenen Webdienste, Skripte, Cookies, etc.
- Zugriff auf **anwaltlich geführte Webdienste & Cookie-Datenbank**.

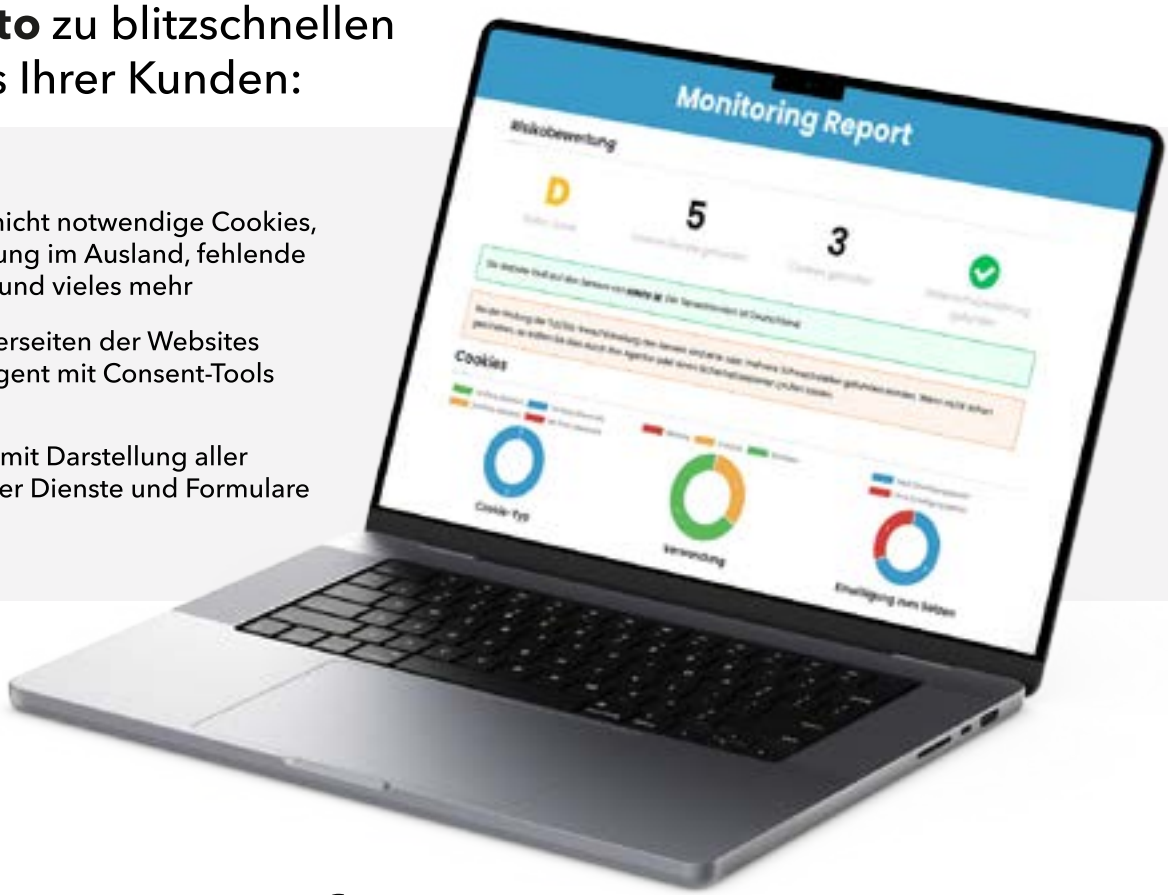
Jetzt kostenfreie Lizenz sichern!
https://website-check.de/dsgvo-guard

Der DSGVO-Guard® ist ein Service der Website-Check GmbH • Beethovenstraße 24 • 66111 Saarbrücken

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.**