Ausgabe 02/2022

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Seite 10

DATENTREUHÄNDER ZWISCHEN DATENSCHUTZ UND DATENNUTZUNG

Louisa Specht-Riemenschneider und Aline Blankertz sehen Treuhänder als Chance, vor allem im Medizinbereich Daten für die Forschung zu nutzen

Seite 16

ADRESSHANDEL UND DIE OFFLINE-WERBUNG IN BRIEFKÄSTEN

Wie die Berliner Aufsichtsbehörde das Aus der Briefwerbung begründet

Seite 40

MIT DEM DIGITAL-FÜHRERSCHEIN FIT FÜRS NETZ

Initiative «Deutschland sicher im Netz» vermittelt Wissen für eine vernetzte Welt

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

www.twitter.com/bvd_datenschutz

www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten

BvD e.V.
DATENSCHUTZ GESTALTEN

Jetzt anmelden: **www.bvdnet.de/herbstkonferenz-datenschutz**

Jetzt Frühbucherrabatt bis 15.08.2022 sichern!

2022

BvD-Herbstkonferenz & Behördentag | 26.10. – 28.10.2022

IM STEIGENBERGER GRAF ZEPPELIN, STUTTGART

WIRTSCHAFT TRIFFT AUFSICHT

DSGVO im 5. Jahr:

WIE HAT DIE EU DEN DATENSCHUTZ VERÄNDERT?

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

THEMEN:

- Ist der Datenschutz nach der Pandemie ein anderer?
- Digitalisierung im Gesundheitswesen
- Neue Handlungsfelder der Datenschutzaufsicht im Rahmen der EU-Digitalgesetzgebung
- Drittstaaten Transfer – FAQs in der aufsichtsbehördlichen Praxis

JETZT ANMELDEN:

www.bvdnet.de/herbstkonferenz-datenschutz

Gemeinsame Konferenz von:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

BayLDA

BvD e.V. DATENSCHUTZ GESTALTEN

Liebe Leserinnen und Leser,

vielleicht ist es Ihnen aufgefallen: Wir haben der BvD-News ein kleines Facelift verpasst. Das letzte liegt bereits einige Jahre zurück, deshalb hielten wir es für an der Zeit, an der einen oder anderen Stelle behutsam zu modernisieren. Die vielleicht deutlichste Neuerung: Die inhaltlichen Rubriken des Magazins sind jetzt jeweils mit einer eigenen Farbe gekennzeichnet, beispielsweise hellblau für Artikel zur Datenschutzpraxis, rot für Berichte „Aus dem Verband" und hellgrün für die Rubrik „Aufsichtsbehörden". Damit wollen wir die Navigation im Heft erleichtern und ein paar frische Farbakzente setzen.

Woran sich in den BvD-News auch in Zukunft nichts ändert, ist die hohe Qualität der Beiträge, die wir unseren exzellenten Autorinnen und Autoren zu verdanken haben. In der vorliegenden Ausgabe sind dies vielfach Referentinnen und Referenten unserer letzten BvD-Verbandstage, die im Mai erstmals wieder als Präsenzveranstaltung in Berlin stattfanden. Einen kurzen Nachbericht dazu finden Sie ebenso in dieser Ausgabe wie zur Premiere unseres Datenschutztages in Frankfurt, den wir Ende Juni gemeinsam mit den Aufsichtsbehörden von Hessen und Rheinland-Pfalz veranstaltet haben.

Eine Frage, die sowohl bei unseren Verbandstagen als auch in diesem Heft mehrfach aufgeworfen wird, ist die nach dem Verhältnis der zahlreichen von der EU geplanten oder jüngst verabschiedeten Rechtsakte aus dem Bereich der Digitalpolitik zur DSGVO. Digital Markets Act, Digital Services Act, Data Act… nicht nur die Menge, auch das Tempo, das die EU-Kommission hier vorlegt, ist beachtlich. Ziel war es dabei die Wettbewerbsmacht der großen Player einzudämmen, europäische Digitalinnovationen zu fördern und so der vielbeschworenen digitalen Souveränität Europas den Boden zu bereiten. Ob das gelingt, schauen wir uns in den nächsten Monaten genauer an.

Diese Gemengelage birgt für uns Datenschutzbeauftragte gleichermaßen Chancen wie Herausforderungen. Denn bei allem „Act"tionismus der EU-Kommission – die DSGVO bleibt „und berührt", wie es in den Verordnungen heißt. Der Datenschutz wird in Europa also auch in Zukunft nicht der Digitalisierung geopfert, und das ist gut so. Doch er wird komplexer, weil eben zukünftig deutlich mehr europäische Verordnungen eine Rolle spielen als nur die DSGVO. Verantwortliche werden von dieser Komplexität überfordert sein und kompetente Beratung benötigen. Die Datenschutzbeauftragten als „Lotsen der Digitalisierung" haben hier die große Chance, mit ihrer Kompetenz noch stärker zu unterstützen – allerdings steigen auch die Anforderungen an die Qualifikation der Datenschutzbeauftragten.

Wir als BvD werden diesen Transformationsprozess im Sinne unseres Berufsstandes begleiten, sowohl durch die umfassende Information und Qualifikation unserer Mitglieder als auch durch politische Arbeit. So werden wir in Kooperation mit der Stiftung Datenschutz, der DIHK und dem Bundesverband der Digitalwirtschaft am 5. September im Haus der Deutschen Wirtschaft in Berlin, zu einer Diskussionsveranstaltung einladen, bei der wir über die aktuelle EU-Regulatorik – insbesondere den Data Act – informieren und diskutieren. Dabei wollen wir durch die „Datenschutzbrille" betrachtet, dafür sensibilisieren, welche rechtlichen und wirtschaftlichen Fragestellungen sich aus dem Data Act in seiner derzeit vorliegenden Entwurfsfassung ergeben. Es ist geplant, die Veranstaltung für Sie auch kostenfrei im Internet zu streamen. Weitere Informationen hierzu finden Sie auf unserer Website. Ich würde mich freuen, wenn Sie dabei sind.

Doch zunächst wünsche ich Ihnen viel Lesevergnügen mit dieser Ausgabe der BvD-News.

Thomas Spaeing
BvD-Vorstandsvorsitzender

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: www.bvdnet.de
www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands
www.linkedin.com/company/berufsverband-der-datenschutzbeauftragten
www.twitter.com/bvd_datenschutz
www.bvdnet.de/feed/

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

Fotos (sofern nicht anderweitig ausgewiesen):
Fotos: 123RF, Adobe Stock,
Fotos Verbandstage Berlin: Dirk Lässig,
Fotos Datenschutztag Hessen & Rheinland-Pfalz sowie Regionatreffen: Christina Denz

Lektorat:
Frank Spaeing, Regina Mühlich

Anzeigen:
Christina Denz
Kooperationen:
Nadja Bunk, Karsten Füllhaase
(bvd-news@bvdnet.de)

Satz, Layout & Produktion:
Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

ISSN: 2194-1025
Erscheinungsweise: 3 x jährlich, Druckauflage 4.000 Exemplare (Unsere Mediadaten erhalten Sie unter bvdnet.de/Publikationen oder von unserer Geschäftsstelle per E-Mail an bvd-gs@bvdnet.de) Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

IM FOKUS

Datenschutz als Innovationsmotor
Datenschutz von Anfang an mitdenken, das macht Produkte, Programme und Systeme effizienter und ressourcenschonender, findet der Bundesdatenschutzbeauftragte.
Prof. Ulrich Kelber 6

Datentreuhänder zwischen Datenschutz und Datennutzung
Den vermeintlichen Gegensatz von Datennutzung und Datenschutz aufheben - besonders im Gesundheitsbereicht - dafür plädieren
Prof. Dr. Louisa Specht-Riemenschneider, Aline Blankertz 10

EU-Digitalgesetzgebung: Wer soll neue Rechtsakte eigentlich umsetzen?
Der BvD denkt auf seinen Verbandstagen im Mai über ein erweitertes Selbstverständnis der Datenschutzbeauftragten nach.
Sebastian Himstedt 14

DATENSCHUTZRECHT

Offline-Werbung in Briefkästen
Die Berliner Datenschutzbeauftragte begründet, wie die DSGVO aus Ihrer Sicht den Adresshandel für Briefkasten-Werbung verbietet.
Annelie Evermann, Giuliana Schreck 16

DATENSCHUTZPRAXIS

Deepfakes made by KI
Künstliche Intelligenz macht Deepfakes überzeugend möglich - und hilft zugleich, solche als Fake zu erkennen.
Nikcolas Müller 20

Datenschutzaudits und Verhaltensregeln
Ein Leitfaden zum aktuellen Stand bei Datenschutzsiegeln.
Stephan Rehfeld, Patrick Grihn, Joachim Ries 24

Datenschutz im Verein – viele offene Fragen für ehrenamtlich Engagierte
Die Stiftung Datenschutz bietet Vereinen Hilfen und Unterstützung beim Datenschutz.
Hendrik vom Lehn 28

AUFSICHTSBEHÖRDEN

Datenherausgabe und Informationsfreiheit by Design
Wie Behörden und Unternehmen sich auf Anfragen nach Datenauskunft vorbereiten können.
Dr. Marit Hansen, Henry Krasemann 34

GESELLSCHAFT

Digitalführerschein macht fit fürs Netz
Deutschland sicher im Netz e.V. vermittelt Wissen rund um die vernetzte Welt.
Dr. Michael Littger 40

AUS DEM VERBAND

“Wer Datenschutz nebenbei machen soll, ist schnell überlastet”
Ein Interview zu den Themen und Herausforderungen behördlicher und kommunaler Datenschutzbeauftragter zum 1. Datenschutztag Hessen & Rheinland-Pfalz. 44

Kritische Stimmen im Glitterregen
Bei der DAME-Preisverleihung holten ein Künstlerkollektiv, zwei Journalisten und ein Schülerprojekt die Trophäen für 2021.
Christina Denz 46

Kurz gefasst
Junge Talente mit Kreativen Ideen für Datenschutz ausgezeichnet 48
Jubiläum beim Datenzirkus 49
Link-Tipp 49
Internationales in der Regionalgruppe Frankfurt 50
Termine der Regionalgruppen und Arbeitskreise 52

REZENSIONEN

Heidelberger Kommentar zum TTDSG 54
Formularhandbuch Datenschutzrecht 56
Datenschutzrecht – Ein Kommentar für Studium und Praxis 57
Praxishandbuch Künstliche Intelligenz 58

PROF. ULRICH KELBER

„DATENSCHUTZ ALS INNOVATIONSMOTOR“

Die beiden vergangenen Pandemiejahre haben unsere Gesellschaft auch digital vor neue Herausforderungen und Aufgaben gestellt. Homeoffice und mobiles Arbeiten sind heute für viele Beschäftigte „normal“. Unternehmen und Verwaltungen haben sich darauf nicht nur sehr schnell sondern teilweise flexibler eingestellt, als man es ihnen zugetraut hätte. Doch erwartet hat das alles vor zwei Jahren sicher niemand. Die Datenschutzaufsichtsbehörden mussten darauf genauso schnell und flexibel reagieren und haben dies auch getan, anders als in manchen Kommentaren und den alltäglichen Talk-Shows dargestellt. Wir Datenschützerinnen und Datenschützer wissen nämlich, dass Datenschutz kein Selbstzweck und Bürokratiemonster, sondern notwendiger Schutz für Menschen, Unternehmen und Verwaltungen ist. Die Digitalisierung macht weltweit große Schritte nach vorne. In Deutschland hinken wir dieser Entwicklung leider ziemlich hinterher. Datenschutz muss hier oft als so falsche wie bequeme Ausrede für mangelnde Geschwindigkeit herhalten. Dabei drängen doch gerade wir Datenschützer auf durchgängige digitale Lösungen.

Deutschland hinkt digital hinterher, aber nicht wegen Datenschutzvorschriften

Deutschland verliert beim Innovations-Tempo im internationalen Vergleich deutlich an Boden. Das ist auch für uns Datenschützer ein Problem. Denn vor allem die Menschen, die wir schützen wollen, sind die Verlierer mangelhafter Digitalisierung. Eine gut umgesetzte digitale Lösung ist aus datenschutzrechtlicher Sicht fast immer besser als die analoge Zettelwirtschaft oder unnötige analoge Dateneinsicht. Der Datenschutz kann seine Aufgabe zum Schutz der verfassungsmäßigen Rechte der Menschen nur dann erfüllen, wenn er selbst Teil der technologischen Entwicklung ist oder mindestens wird.

Deutschland ist im Ländervergleich des jüngsten Global Innovation Index der UN-Organisation für geistiges Eigentum zurückgefallen. Bei der digitalen Beteiligung der Bevölkerung rutschte Deutschland von Platz 23 im Vorjahr auf Platz 57 ab, bei Digitalangeboten der öffentlichen Verwaltung sogar von Platz 17 auf Platz 59. Übrigens liegen viele Staaten mit dem gleichen Datenschutzrecht, der europäischen Datenschutzgrundverordnung, vor uns in der Rangliste. Ich kann mich der Präsidentin des Deutschen Patentamts, Cornelia Rudloff-Schäffer, nur anschließen, dass die digitale Transformation und das Bewusstsein für die Dringlichkeit ihres Vorantreibens in unserer Gesellschaft noch nicht so ausgeprägt ist, wie in anderen Teilen der Welt. Und ebenso ihrer Schlussfolgerung: „Etwas mehr Dynamik würde unserer Innovationslandschaft guttun.“

Dazu brauchen wir hier deutlich mehr weltmarktfähige Produkte. Datenschutz darf angesichts dieser Defizite nicht als Ausflucht dienen die Digitalisierung zu verschleppen. Im Gegenteil: Datenschützerinnen und Datenschützer müssen noch frühzeitiger beraten und prüfen – wenn man uns denn liesse. Die Corona-Krise hat längst bekannte Schwächen bei der Digitalisierung schonungslos offengelegt. Was vor Corona nicht geklappt hat, ist mit Corona implodiert: Fehlende WLAN-Anschlüsse, antike Endgeräte, mangelnder Austausch oder Zuständigkeitswirrwar. Das Beispiel der klappernden Faxgeräte in den Gesundheitsämtern, womöglich noch mit Thermopapier, kennen wir alle doch schon lange. Die öffentliche Gesundheitsvorsorge ist über viel Jahre hinweg kaputtgespart worden. Diese Versäumnisse haben sich in der Pandemie bitter gerächt. Ich bin einfach nur entsetzt darüber, dass bis Ende 2021 gerade einmal 16 von insgesamt 575 Verwaltungsleistungen für die Bürgerinnen und Bürger bundesweit online verfügbar waren. Bund, Länder und Kommunen haben sich zwar vorgenommen auf der Grundlage des Onlinezugangsgesetzes bis Ende 2022 alle 575 Behördenleistungen zu digitalisieren. Ehrgeizige Ziele, doch wer von uns glaubt, dass dieser Endspurt noch zu schaffen ist?

Deutsche Politik hat sich viel vorgenommen

Der unabhängige Nationale Normenkontrollrat, der die Bundesregierung seit 2006 beim Bürokratieabbau berät, hält dieses Ziel für nicht mehr erreichbar. Auch der Deutsche Städte- und Gemeindebund warnte vor einem Scheitern der Regierungspläne für die Digitalisierung der Verwaltungen. Hier kommt auf die aktuelle Bundesregierung einiges zu. Und sie hat sich selbst noch mehr vorgenommen: Ein Transparenzgesetz, ein Umweltdatenportal, einen Digitalisierungscheck für alle Gesetzesvorhaben, eine souveräne Bundescloud, den Umbau der Sicherheitsarchitektur, ein Datengesetz und ein Dateninstitut, ein Beschäftigtendatenschutzgesetz, ein Forschungsdatengesetz, einen Datenraum Mobilität und ein Register- und Gesundheitsdatengesetz. Und selbst das sind nur einige wenige Verabredungen aus dem Koalitionsvertrag. Ich kann nur hoffen, dass sie dabei nicht den Fehlern einiger Digitalisierungsversager aus den Vorjahren folgen und den

Schwarzen Peter an den Datenschutz und andere schieben. Ich hoffe sehr, dass sie die tatsächlichen Probleme angehen und Lösungen finden. Meine Behörde und ich stehen jedenfalls für die Beratung bereit, aber eben auch für die Prüfung. Das gilt ebenfalls für die nationale Umsetzung der vielfältigen europäischen Rechtsetzungsakte wie Data Act, Data Governence Act, Digital Markets Act, Digital Services Act, KI-Regulierung, ePrivacy-Verordnung und Data Spaces.

Datenschutz ist gelebter Grundrechtsschutz und wichtiger Vertrauensanker für die Digitalisierung unserer freiheitlichen Gesellschaft. Damit hat Digitalisierung eine enorme wirtschaftspolitische Dimension. Hier geht es darum Prozesse durch die Digitalisierung effizienter zu gestalten. Aber es geht zum Beispiel auch darum im produzierenden Gewerbe völlig neue Wege zu beschreiten. Um perspektivisch viel kundenspezifischer, termingerechter und ressourcenschonender zu produzieren.

All diese Systeme müssen „Daten"-sicher sein. Denn es stellen sich neue Herausforderungen, etwa mit Blick auf das Thema Industriespionage und Sabotageschutz. Ohne starken Datenschutz und ein hohes Maß an Datensicherheit steigen die Risiken hierfür massiv an. Gerade im ,,Land der Entwickler" und der vielen kleinen und mittelständischen Unternehmen, die mit ihren Ideen „hidden Champions" sind, wäre ein Know-how- und Wissensabfluss existenzbedrohend. Wenn Produktionsabläufe und Arbeitsverfahren digitalisiert werden, ist man gut beraten die genutzten IT-Systeme bestmöglich zu schützen.

Es gilt mein Dauercredo: Datenschutz und Datensicherheit müssen bei der Entwicklung und Entstehung neuer Produkte, Programme und Systeme von Anfang an mitgedacht und mitentwickelt werden. Das ist kostengünstiger, sicherer und ressourcenschonender. Das schützt nicht nur Menschen, sondern auch Ideen, Patente, Wissen, Verfügbarkeit, Glaubwürdigkeit und noch so viel mehr. Wie positionieren sich Deutschland und Europa also in dieser vernetzten Welt? Wir treten auf der Stelle! Asien und die USA betrachten Europa technologisch zunehmend in immer mehr Bereichen im Rückspiegel. Europa wird zum reinen Absatzmarkt digitaler Services. Wir haben es bisher selbst kaum geschafft weltweit agierende IT- und Internetunternehmen hervorzubringen. Wir sollten uns fragen, woran das liegt, auch um werthaltige Arbeitsplätze in Europa zu sichern.

Der erste Reflex bei manchen dürfte ein Wort sein: Datenschutz! Diese haltlose Behauptung ist zwar nicht wirklich neu. Sie wird allerdings mittlerweile so oft genutzt, dass es beinahe schon selbst eine kleine Pandemie geworden ist. Mehr technischer Sachverstand und mehr Ehrlichkeit bei den wahren Gründen für Digitalisierungsversagen wäre der einzige Impfstoff dagegen. Wenn es nicht so gefährlich wäre, würde

Prof. Ulrich Kelber auf den BvD-Verbandstagen 2022 in Berlin.

ich das Ganze nur noch genervt hinnehmen. Weil die Behauptung aber nicht mehr überwiegend auf Unwissen beruht, sondern gezielt als Falschinformation eingesetzt wird, müssen Datenschützer immer wieder klar Stellung beziehen.

Datenschutz hat bis heute nachweislich keine einzige geeignete Maßnahme zur Pandemiebekämpfung verhindert! Datenschutz ist keine heilige Kuh, die über allem anderen steht. Und Datenschutz ist kein Wirtschaftshemmnis und damit auch nicht der Sargnagel der deutschen Unternehmen. Datenschutz könnte vielmehr Innovationsträger und Wettbewerbsvorteil sein, wenn Unternehmen und Behörden sich darauf einlassen. Unser Ziel in Deutschland und Europa sollte es sein weltweit Marktführer bei sicheren und datenschutzkonformen Produkten und Dienstleistungen zu werden. Datenschutzkonforme Produkte „made in Europe" könnten sich als positives Differenzierungsmerkmal am Markt etablieren.

Mit Blick auf den Datenschutz haben wir in Europa einen Erkenntnis-, einen Regelungs- und damit Wettbewerbsvorteil. Diese Potenziale müssen wir nutzen und positiv vermarkten. Wir verfügen mit der Datenschutzgrundverordnung und unserem nationalen Datenschutzrecht über einen innovativen Rechtsrahmen mit klaren Leitplanken und Handlungsanweisungen. Um diesen Rechtsrahmen werden wir beneidet. Die Datenschutzgrundverordnung wird weltweit als Referenz und Blaupause für eigene Rechtsvorgaben herangezogen, in Korea, Japan, Mexiko, Indien und in mehreren US-Bundesstaaten. Zuletzt sogar in China, wenn auch aus anderen Gründen.

Datenschutz und IT-Sicherheit gehen Hand in Hand

Es kann doch nicht sein, dass jetzt ausgerechnet US-Unternehmen, mehr oder weniger glaubwürdig, Datenschutz massiv als Unterscheidungsmerkmal zur Konkurrenz bewerben, während die Vertreter der deutschen Wirtschaft darüber klagen, dass sie ein Grundrecht einhalten müssen. Die Grundsätze des Datenschutzes durch Technikgestaltung („Data Protection by Design“) und der datenschutzfreundlichen Voreinstellungen („Data Protection by Default“) sind ein wichtiger Bestandteil der Datenschutzgrundverordnung. Außerdem muss der Grundgedanke der Herstellerhaftung ins Datenschutzrecht übertragen werden. Letztendlich gilt: Es kann IT-Sicherheit ohne Datenschutz geben, aber es gibt keinen Datenschutz ohne IT-Sicherheit. Eine funktionierende IT-Sicherheit ist eine grundlegende Voraussetzung für einen funktionierenden Datenschutz. Datenschutz braucht nicht nur IT-Sicherheit, sondern er setzt ihr auch Grenzen.

Da nämlich IT-Sicherheitsmaßnahmen in der Regel die Verarbeitung personenbezogener Daten umfassen, müssen sie selbst so gestaltet sein, dass der Datenschutz in diesem Zusammenhang gewahrt bleibt. Der Verantwortliche muss Vertraulichkeit, Integrität und Verfügbarkeit der Verarbeitung sicherstellen. Das sind die bekannten Grundwerte der Informationssicherheit. Außerdem muss der Verantwortliche Maßnahmen ergreifen, um die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem Zwischenfall rasch wiederherzustellen. Auch wenn das Stichwort selbst nicht wörtlich in der DSGVO steht, so ist es doch relativ klar, dass damit ein Notfallvorsorgekonzept gemeint ist. Denn ohne entsprechende Maßnahmen im Vorfeld eines Zwischenfalls ist der Versuch einer raschen Wiederherstellung in der Regel zum Scheitern verurteilt.

Schließlich fordert der Artikel 32 DSGVO vom Verantwortlichen noch explizit ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen umzusetzen. Das heißt: ein IT-Sicherheitsmanagement. So stellt die DSGVO eine Verbindung zwischen Datenschutz und IT-Sicherheit her. Bei allen Gemeinsamkeiten und möglichen Synergieeffekten gibt es trotzdem Unterschiede: Risiken aus der IT-Sicherheit beziehungsweise aus dem IT-Sicherheitsmanagement sind Risiken für die Organisation, die die Daten verarbeitet. IT-Sicherheitsvorfälle können zu Schäden für die Organisation führen, deren Eintrittswahrscheinlichkeit und Höhe das Risiko bestimmen; Schäden aus diesem Bereich sind letztlich eigentlich immer finanzielle Schäden. Für solche Risiken gibt es Berechnungsmodelle, die einen Wert liefern, mit dem das Risiko eben „bewertet“ werden kann.

Die DSGVO spricht hingegen von den Risiken für die Rechte und Freiheiten natürlicher Personen. Der Unterschied ist in diesem Fall wirklich nicht fein, sondern grundlegend. Denn die „Träger“ des Risikos sind andere: Es sind die Personen, deren Daten verarbeitet werden – in der Terminologie der DSGVO die „betroffenen Personen“. Sie haben keinen Einfluss darauf, wie ihre Daten verarbeitet werden und welche Maßnahmen der Verantwortliche gegebenenfalls zu ihrem Schutz umsetzt. Es geht hier also ganz konkret um Menschen.

FAZIT

Als Informatiker weiß ich, dass digitale Lösungen in der Regel viel datenfreundlicher sind als die analogen. Niemand muss mich überzeugen, dass die Digitalisierung enorme Vorteile mit sich bringt und weiter bringen wird. Aber es muss eben auch jedem klar sein, dass nicht jede Neuerung tatsächlich auch innovativ und gesetzeskonform ist. Die Potenziale der Digitalisierung müssen wir zum Wohle Aller und für eine gute gesellschaftliche und wirtschaftliche Zukunft nutzen. Eine „menschenfreundliche“ Gestaltung digitaler Geschäftsmodelle von Anfang an ist hierfür wichtig und machbar. Wir müssen die Chancen der Digitalisierung nutzen und dabei unsere europäischen Werte bewahren.

Datenschutz und Datensicherheit betrifft eben nicht nur die Menschen in unserem Land, sondern ist auch für Verwaltungen und Unternehmen von zentraler Bedeutung. Wir müssen sicherstellen, dass die Digitalisierung alle mitnimmt und für alle sichergestellt ist, dass kein Missbrauch mit Daten stattfindet. Vertrauen ist hier von zentraler Bedeutung, für die Menschen wie für die Wirtschaft und Verwaltung. Die Datenschutzaufsichtsbehörden stehen für diesen Prozess als Partner mit Beratung und Prüfung zur Seite.

Über den Autor

Prof. Ulrich Kelber
ist seit 2019 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.

▶ www.bfdi.bund.de

BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Jetzt 3 Monate ZD kostenlos testen und Geschenk sichern!

IHR GESCHENK

SONDERAUSGABE DER AUSKUNFTS-ANSPRUCH NACH ART. 15 DS-GVO

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.

ZD – Zeitschrift für Datenschutz

11. Jahrgang. 2021. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 279,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 219,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 15,– jährlich.

beck-shop.de/go/ZD

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

C.H.BECK

DATENTREUHÄNDER ZWISCHEN DATENSCHUTZ UND DATENNUTZUNG

Prof. Dr. Louisa Specht-Riemenschneider, Aline Blankertz

Wie sich im Gesundheitsbereich Daten für Forschung nutzen ließen ohne den Datenschutz preiszugeben.

Die Datenökonomie betrachtet Daten nicht nur aus der datenschutzrechtlichen Perspektive, sondern ebenso als einen wirtschaftlich und gesellschaftlich relevanten Produktionsfaktor. Daten können einen erheblichen gesellschaftlichen Mehrwert schaffen, zum Beispiel wenn sie bei der Auswahl der am besten geeigneten Therapie helfen und so die Gesundheitsversorgung verbessern oder Entscheider darüber informieren, wo und wie in einer Wertschöpfungskette am effizientesten CO2 eingespart werden kann. Allerdings ist die Datennutzung momentan oft unzureichend und führt zu einer Unternutzung von Daten.[1] Das trifft auch auf die Datennutzung innerhalb von Unternehmen zu, doch erst recht auf die Nutzung zwischen mehreren Unternehmen, denn freiwilliges Datenteilen findet bislang in einem nur sehr begrenzten Umfang statt. 74 Prozent von über 500 im Rahmen einer Studie befragten Unternehmen halten eine Datenweitergabe an andere Unternehmen für „nicht erwünscht". 85 Prozent der befragten Unternehmen sehen datenschutzrechtliche Grauzonen und 84 Prozent „Unklarheiten bezüglich der Nutzungsrechte an den Daten" als ausschlaggebend für das nicht erfolgende Datenteilen.[2]

Doch Datennutzbarkeit und Datenschutz stehen sich nicht derart unversöhnlich gegenüber, wie man bislang den Eindruck hat. Die in der Datenschutzgrundverordnung niedergelegten Grundsätze sind wichtiger Bestandteil einer europäischen Werteordnung. Das bedeutet nicht, dass das Datenschutzrecht alleiniger Orientierungspunkt im Umgang mit Daten sein sollte. Im Gegenteil bestehen neben dem Schutz des informationellen Selbstbestimmungsrechts weitere ebenso schützenswerte Interessen, wie etwa die Forschungsfreiheit und der damit verbundene gesellschaftliche Erkenntnisgewinn, für den eine erhöhte Datennutzbarkeit beispielsweise durch Auswertung großer Datenbestände durchaus dienlich wäre.

Datentreuhandmodelle können ein Weg sein, um die vermeintliche Gegensätzlichkeit von Datennutzung und Datenschutz aufzuheben, da sie unter anderem erlauben Erkenntnisse aus Daten zu gewinnen ohne vertraulich zu behandelnde Informationen preiszugeben. Insbesondere im Gesundheitssektor erscheint das Potenzial der ungenutzten Daten aktuell besonders groß, was sich in diversen politischen Initiativen widerspiegelt, um mehr Datennutzung zu ermöglichen. Allerdings unterscheiden sich diese Initiativen oft hinsichtlich ihrer Zweckbeschreibung, was wiederum unterschiedliche Anforderungen an die Datentreuhänder nach sich zieht. Die Ausgestaltung von Datentreuhändern muss maßgeblich entsprechend ihrem Zweck erfolgen.[3]

[1] Schätzungen zufolge werden 60-95% der erhobenen Daten nicht verwendet, um aus ihnen Informationen zu gewinnen.
[2] Institut der deutschen Wirtschaft (2021): Datenwirtschaft in Deutschland, S. 40.
[3] Specht-Riemenschneider, L., Kerber, W. (2022): Datentreuhänder – Ein problemlösungsorientierter Ansatz, Konrad-Adenauer-Stiftung.

Im Weiteren systematisieren wir verschiedene Datentreuhandmodelle und beschreiben, welche davon insbesondere im Gesundheitsbereich in der Entwicklung sind.

Definition der Datentreuhand

Bisher gibt es keine allgemein akzeptierte Definition von Datentreuhändern. Da der Begriff momentan sehr breit verwendet wird, ist es sinnvoll eine diese Verwendungen erfassende Mindestdefinition für Datentreuhänder zu entwickeln, die sich anschließend in Grundmodelle aufspalten und zum Beispiel nach Sektoren weiter spezifiziert werden kann.

Wir verstehen den Begriff der Datentreuhand zunächst als Oberbegriff sämtlicher Modelle, die heute als Datentreuhand gedacht werden. Die möglichen Ziele und Zwecke einer Datentreuhand sind vielfältig und umfassen u.a. Datenverwaltung mit Unparteilichkeit und/oder Loyalität, Stellung als Vertrauensanker zwischen Datengebenden und Datennutzenden, Ausschluss von unbefugtem Datenzugriff, Erfüllung von Datenschutzbestimmungen und/oder Stärkung, Gewährleistung oder Wiederherstellung individueller oder kollektiver Kontrolle über Daten.[4]

Aus diesen Zielen lassen sich folgende drei Anforderungen an eine Datentreuhand ableiten:

- **Datenintermediär:**
  Eine Datentreuhand übernimmt zumindest auch eine Funktion der Datenzugangsmittelung, darüber hinaus möglicherweise auch die Datenverwaltung, -durchleitung und/oder -aufbereitung zum Nutzen einer anderen Partei (oder mehrerer).
- **Erfüllung rechtlicher Anforderungen:**
  Eine Datentreuhand ist mindestens an den bestehenden Rechtsrahmen gebunden. Das heißt, ihre Aktivitäten erfüllen sowohl allgemeine rechtliche Anforderungen (zum Beispiel Datenschutz, Kartellrecht) als auch spezifisch ausgestaltete Vereinbarungen zwischen beteiligten Parteien in Form eines Vertrags.
- **anwendungsabhängige Vertrauens-/Neutralitätsanforderungen:**
  Je nach Einsatzbereich einer Datentreuhand können unterschiedliche Mechanismen sinnvoll und geboten sein, um Vertrauen/Neutralität und eine wünschenswerte Verteilung des aus Daten gewonnenen Wertes zu erzielen. Aufgrund der Vielfalt möglicher Ziele sind diese Anforderungen nicht allgemein sondern in Abhängigkeit von Anwendungsfällen zu bestimmen.

AUS DER ABLEITUNG ERGIBT SICH FOLGENDE DEFINITION:

> Eine Datentreuhand ist eine natürliche oder juristische Person oder eine Personengesellschaft, die den Zugang zu von Datentreugebern bereitgestellten oder bereitgehaltenen Daten nach vertraglich vereinbarten oder gesetzlich vorgegebenen Data-Governance-Regelungen im Fremdinteresse mittelt.

Systematische Unterscheidung nach Zentralität und Freiwilligkeit

Es lassen sich aus diesem Oberbegriff vier Grundmodelle mit unterschiedlichem Risikopotenzial entwickeln, das jeweils maßgeblich für die Regulierungsintensität sein sollte:

Zentral oder dezentral: Eine zentrale Datenspeicherung ist mit höheren Risiken verbunden. Dabei ermöglicht sie allerdings zusätzliche Formen der Datennutzung und stellt zugleich höhere Anforderungen an die zugrundeliegende Infrastruktur. So verspricht die zentrale Speicherung beim Datentreuhänder eine einfachere Verwaltung der Daten durch ebendiesen. Weitergehende Befugnisse sind möglich, wie zum Beispiel auch den Datenverarbeiter vom Zugang auszuschließen. Die Datentreuhand kann im Falle einer zentralen Speicherung die Daten umfassend nutzen (zum Beispiel analysieren) oder verändern (zum Beispiel löschen). Wenn eine Datentreuhand Daten anonymisiert oder pseudonymisiert, können Originaldaten dezentral gehalten werden und eine Datentreuhand kann zentral Zugang zu den entsprechend anonymisierten oder pseudonymisierten Daten an (vertraglich definierte) Dritte gewähren.

Freiwillig oder verpflichtend: Als Ausgangspunkt wird allgemein angenommen, dass Beteiligte frei sind in ihrer Entscheidung, ob sie eine Datentreuhand nutzen wollen, sofern nicht besondere Gründe vorliegen, die eine Verpflichtung begründen. Bei freiwilliger Nutzung lässt sich die Datentreuhand über einen Datentreuhandvertrag regeln, der die recht-

[4] Blankertz, A., Braunmühl, P.V., Kuzev, P., Richter, F., Richter, H., Schallbruch, M. (2020): Datentreuhandmodelle – Themenpapier, verfügbar unter: https://www.stiftung-nv.de/sites/default/files/20200428-datentreuhandmodelle.pdf

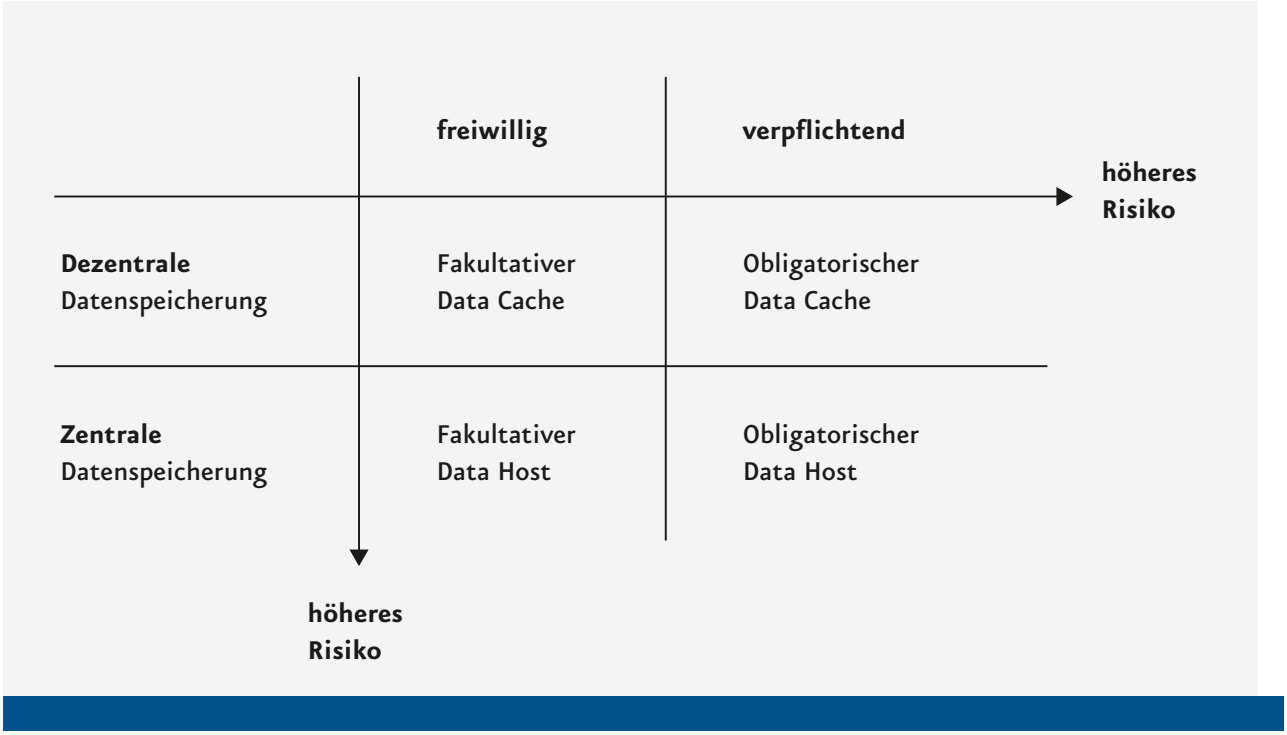
liche Grundlage des Datenaustauschs darstellt.[5] Eine Pflicht zur Nutzung einer Datentreuhand hingegen kann dadurch begründet werden, dass das Ziel durch freiwillige Maßnahmen nicht zu erreichen ist. Zudem muss das Ziel eine regulatorische Intervention rechtfertigen. Hier können verschiedene Faktoren eine Rolle spielen, darunter ein ausgeprägtes öffentliches Interesse an dem mit der Datentreuhand verfolgten Ziel oder eine hohe Konzentration auf einem der an der Datentreuhand beteiligten Märkte bzw. ein deutliches Ungleichgewicht zwischen den Beteiligten, sodass Verhandlungsmacht überwiegend bei einer Partei liegt.

Datentreuhandmodelle im Gesundheitssektor

Das Potenzial von Daten, um beispielsweise eine Diagnose zielsicherer zu machen oder Wechselwirkungen zwischen Krankheiten oder zwischen Therapien zu erkennen, ist enorm. Dies erklärt das große Interesse daran Gesundheitsdaten breiter verfügbar zu machen. Gleichzeitig sind Gesundheitsdaten hochsensibel und können nicht in Rohform offen zur Verfügung gestellt werden. Es gibt vielfältige Bestrebungen, um die Daten besser zu nutzen; diese unterscheiden sich wiederum klar in Bezug darauf, welche Ziele sie im Konkreten verfolgen und daher auch, welche Form von Datentreuhand sie umsetzen.

Mit der elektronischen Patientenakte (ePA) erhalten Patientinnen und Patienten ein Instrument, um Daten über sich zwischen den sie behandelnden Gesundheitsdienstleistern – niedergelassene Ärztinnen/Ärzte, Apotheken oder Krankenhäuser – zu teilen oder granular zu steuern, welche Behandelnden welche Daten erhalten. Das Ziel besteht primär darin Daten über die einzelnen Patientinnen und Patienten aus verschiedenen Quellen besser miteinander zu vernetzen und nicht diese über Patientinnen und Patienten hinweg zu analysieren. Wenn Daten geteilt werden, sind diese zwangsläufig personenbezogen, da keine personenübergreifende Analyse vorgesehen beziehungsweise erwünscht ist. Die ePA ist somit dezentral konstruiert. Da der Nutzen direkt den Einzelnen zugute kommen soll, ist sie freiwillig: Versicherte sind frei sich gegen die Verwendung der ePA zu entscheiden bzw. bestimmte Datenpunkte einzuspeisen und zu teilen.

Anders verhält es sich beispielsweise bei dem Forschungsdatenzentrum (FDZ) Gesundheit oder dem Transplantationsregister, die zumindest teilweise einen zentralen und verpflichtenden Ansatz wählen. Das FDZ Gesundheit soll die Analyse von



Risikobasierte Unterscheidung von Datentreuhandmodellen

[5] Specht-Riemenschneider, L., Blankertz, A. et al. (2021): Die Datentreuhand, MMR-Beilage, 25.

[6] Siehe Webseite des FDZ, https://www.forschungsdatenzentrum-gesundheit.de/das-fdz

pseudonymisierten Abrechnungsdaten der gesetzlich Krankenversicherten ermöglichen, um darauf aufbauend die allgemeine Gesundheitsversorgung zu verbessern. Dazu soll es „virtuelle Analyseräume“[6] geben, was mit data-clean rooms gleichbedeutend sein kann, in denen Forschende Analysen durchführen und Ergebnisse erhalten ohne direkten Zugriff auf die Daten zu benötigen. Beim Transplantationsregister werden Daten spezifisch über Transplantationen erhoben, die pseudonymisiert für Forschung verwendet werden können. Darüber hinaus haben Patientinnen und Patienten die Möglichkeit in die Verwendung ihrer personenbezogenen Daten einzuwilligen. Zudem gibt es Bestrebungen deutlich umfangreichere Datensätze aus der Interaktion von Behandelnden und Patientinnen und Patienten zu analysieren. Diese fokussieren üblicherweise zunächst auf bestimmte Bereiche, in denen umfangreiche Forschungsdatensätze aufgebaut und zur Verbesserung der Diagnose und Therapie werden sollen. Ein Beispiel ist RACOON, das radiologische Daten und Befunde von allen deutschen Universitätskliniken vernetzt und sie für ein Echtzeit-Monitoring von Covid-19-Verläufen sowie für die Verfeinerung der bestehenden Diagnosemöglichkeiten nutzbar machen soll. Das zugrundeliegende Datentreuhandmodell verbindet dezentrale und zentrale Elemente. Einen ähnlichen Ansatz verfolgt auch die Medizininformatik-Initiative (MII), die ebenfalls eine institutionsübergreifende Datenauswertung anstrebt. Allerdings zeigt sich hier eine Herausforderung für Initiativen dieser Art, da eine Einwilligung auch für die Verwendung pseudonymisierter Daten aufwändig zu erheben ist: Die MII hat einen Mustertext für die Patienteneinwilligung entwickelt,[7] der eine breitere Einwilligung in die Nutzung von Daten für Forschung ermöglichen soll, ohne dass die Zwecke im Detail spezifiziert wären. Der Text umfasst jedoch sieben Seiten Aufklärung und vier Seiten für die Einwilligung, sodass das Formular bisher nur sehr begrenzt in die klinische Praxis übernommen wurde und unklar ist, ob dies noch umfassender geschieht.

Somit zeigen sich alle Ausprägungen von Datentreuhandmodellen im Gesundheitssektor: Bei der ePA, die zunächst die Versorgung des/der Einzelnen verbessert, ist ein dezentraler, rein freiwilliger Ansatz zielführend. Bei Forschungsgebieten mit klarem Nutzen für das Gemeinwohl wie Transplantationen erfolgt die zentrale Sammlung von pseudonymisierten Daten zunächst automatisch und kann von Patientinnen und Patienten durch eine Einwilligung um personenbezogene Daten ergänzt werden. Verknüpfungen von umfassenden Datensätzen, um zum Beispiel Bilddaten übergreifend zu analysieren, befinden sich in der Entwicklung und werfen Fragen auf, inwiefern umfangreiche Einwilligungen für die Verwendung pseudonymisierter Datensätze tatsächlich sinnvoll sind.

Die Verbindung von Datenschutz und Datennutzbarkeit im Forschungsinteresse

Angesichts des großen Potenzials von Gesundheitsdaten erscheint es unangemessen, Rechtsunsicherheit über Datenaustausch als Hemmnis hinzunehmen. Die Datenschutzgrundverordnung verhindert hier die Datennutzung nicht – ganz im Gegenteil lässt sie dem Gesetzgeber insb. nach Art. 9 Abs. 2 lit h – j DSGVO Möglichkeiten die Datennutzbarkeit im Einklang mit dem Datenschutzrecht rechtssicher auszugestalten. Eine solche Möglichkeit, Datenschutz und Datennutzbarkeit rechtssicher miteinander zu verbinden, bietet die Datentreuhand, die Zugang zu den bei verschiedenen Stellen gespeicherten Daten bekommen und die einen sicheren Raum zur Datenauswertung bieten könnte. Sie könnte durch entsprechende technische und rechtliche Ausgestaltung die Datenverarbeitung so sicher erscheinen lassen, dass das Risiko für die Rechte und Freiheiten des Einzelnen und damit auch das gesamtgesellschaftliche Risiko der Datennutzung gering ist. Dies erlaubt es, die Datenverarbeitung in der Datentreuhand auch gesetzgeberisch gegenüber dem realen Datenteilen zu privilegieren. Der nationale Gesetzgeber könnte und sollte daher zügig einen Erlaubnistatbestand zur Verarbeitung auch von sensiblen Daten zu Zwecken der wissenschaftlichen Forschung i.S.d. Art. 9 Abs. 2 lit. h – j DSGVO durch einen Datentreuhänder z.B. in dem im Koalitionsvertrag angekündigten Datentreuhandgesetz schaffen.

Über die Autorinnen

Prof. Dr. Louisa Specht-Riemenschneider
hält den Lehrstuhl für Bürgerliches Recht, Informations- und Datenrecht an der Friedrich-Wilhelms-Universität Bonn. Dort leitet sie auch die Forschungsstelle für Rechtsfragen neuer Technologien sowie Datenrecht. Zuvor lehrte und forschte sie unter anderem an der Universität Passau zu europäischem und internationalem Daten- und Informationsrecht. Ihre Arbeiten wurden mehrfach ausgezeichnet.

Aline Blankertz
ist angewandte Ökonomin mit einem Schwerpunkt auf Daten und digitalen Märkten. Aktuell ist sie Co-Chair der SINE Foundation, eines gemeinnützigen Think-and-Do-Tank für Datenkollaborationen; davor war sie u.a. bei der Sitftung Neue Verantwortung und in der wirtschaftswissenschaftlichen Beratung tätig.

[7] Verfügbar unter: https://www.medizininformatik-initiative.de/sites/default/files/2020-04/MII_AG-Consent_Einheitlicher-Mustertext_v1.6d.pdf

SEBASTIAN HIMSTEDT

EU-DIGITALGESETZGEBUNG: WER SOLL NEUE RECHTSAKTE EIGENTLICH UMSETZEN?

Der BvD denkt auf seinen Verbandstagen in Berlin über eine neue Rolle für Datenschutzbeauftragte nach.

Während die einen über nichts anderes mehr diskutieren, sind die neuen europäischen Rechtsakte wie Digital Services Act (DSA), Digital Markets Act (DMA) oder der noch am Anfang stehende Data Act noch gar nicht im Bewusstsein anderer Datenschutzbeauftragter angekommen. Kein Wunder, heißt es doch beispielsweise im DSA, „dieser Vorschlag lässt die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung) und andere Unionsvorschriften zum Schutz personenbezogener Daten und der Privatsphäre in der Kommunikation unberührt." Doch was bedeutet das in der praktischen Anwendung: Wie relevant sind diese Rechtsakte für Unternehmen und wer sorgt für ihre Umsetzung? Diese offenen Fragen waren für den Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. Grund genug auf den endlich wieder in Präsenz stattfindenden BvD-Verbandstagen am 10. und 11. Mai in Berlin diesen Gesetzgebungsverfahren breiten Raum zu geben.

Besonders am zweiten Tag der mit rund 200 Teilnehmenden besuchten Verbandstage sprachen viele Expertinnen und Experten über die aktuellen digitalpolitischen Entwicklungen auf europäischer Ebene: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Prof. Dr. Dieter Kugelmann, gab einen Überblick über den Datenschutz im digitalen EU-Binnenmarkt, Jana Gooth, wissenschaftliche Referentin der Grünen-EU-Parlaments-Abgeordneten Alexandra Geese, begeisterte das Plenum mit Insights aus dem Gesetzfindungsprozess zum Digital Services Act.

Zum anstehenden Data Act adressierte Dr. Christoph Ritzer, Partner bei der Großkanzlei Norton Rose Fulbright, die noch offenen Fragen in der Gesetzgebung. Konkret fragte Ritzer, wie Unternehmen mit personenbeziehbaren Daten umgehen sollen, wenn es im Data Act keine Rechtsgrundlage aus der DSGVO gibt, diese aber natürlich weiterhin und unmittelbar gilt? Wer überwacht das? Um welche Arten von Daten handelt es sich eigentlich, die ein Connected Car produziert, wenn man diese doch immer auf den Fahrer rückverfolgen und somit ein Bewegungsprofil erstellen kann? Zu diesem Zeitpunkt, zu dem nur ein erster Entwurf des Data Act vorliegt, gibt es darauf noch keine Antwort.

Dr. Chistoph Ritzer von Norton Rose Fulbright gab auf den BvD-Verbandstagen im Mai 2022 einen Überblick über geplante und fast realisierte EU-Vorhaben zum Thema Datenschutz.

Grundlegend wird im praktischen Alltag jedoch nicht allein zu entscheiden sein, ob es sich um einen Vorgang nach DSGVO handelt oder nicht, sondern darum gehen ein ganz neues Verständnis vom Umgang mit Daten zu erlangen. Denn wenn die Datennutzung zur Schaffung von Innovationen dienen soll, müssen die geeigneten Vorkehrungen – technisch und rechtlich – getroffen werden, um Daten sowohl zu sichern als auch zu schützen. Sonst geht der vermeintliche Wettbewerbsvorteil flöten. In seiner Eröffnungsrede ging der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Prof. Ulrich Kelber, genau darauf ein und warb für einen innovationsoffenen, aber sicheren Umgang mit Daten. Denn „nicht Daten sind die neue Währung, sondern Vertrauen", sagte Kelber. Um dies zu erreichen, müsse „Datenschutz in die DNA der Produkte einfließen", also schon bei der Entwicklung mitgedacht werden. Für Datenschutzbeauftragte in Unternehmen und öffentlichen Stellen bedeute dies, dass sie von Anfang an mit eingebunden

werden müssten und nicht erst am Ende des Prozesses, kurz vor der geplanten Einführung, forderte Kelber.

In der abschließenden Panel-Diskussion brachte BvD-Vorstandsvorsitzender Thomas Spaeing einen Vorschlag in die Debatte ein, der die Rolle der Datenschutzbeauftragten in den Blick nimmt. Um zu unterscheiden, welche Daten unter die unterschiedlichen Rechtsakte, insbesondere den Data Act, fallen und im Sinne einer Datenteilung weitergegeben werden könnten, sollte die Rolle der Datenschutzbeauftragten überdacht und erweitert werden. Aber auch im Umgang mit dem DSA wird es darum gehen die Prozesse mit der zuständigen Stelle, dem neuen Koordinator für digitale Dienste, abzustimmen – so wie es sich in der Vergangenheit gut etabliert hat die Kommunikation mit den Datenschutzaufsichtsbehörden über den Datenschutzbeauftragten abzudecken.

So wie sich der Umgang mit Daten in der Datenökonomie wandelt, so wird sich also die Arbeit des Datenschutzbeauftragten erweitern müssen. Aus Sicht von Spaeing ist die gute Nachricht, dass diese Personen schon vielfach vor Ort und „seit jeher gut ausgebildete Ansprechpartner“ sind. In Zusammenarbeit mit den Fachabteilungen könnten die Datenschutzbeauftragten gerade kleine und mittelständische Unternehmen in die digitale Zukunft begleiten.

Datenschützer mögen sich schon deshalb damit befassen, weil die Betroffenen geschützt werden müssen, aber es auch im Interesse der Verantwortlichen ist, insbesondere im Mittelstand. Oftmals ist nämlich der Datenschutzbeauftragte der einzige im mittelständischen Unternehmen, der das nötige Know-how in diesem Bereich mitbringt. Und damit nicht andere darüber entscheiden, welche Daten in welcher Weise das Unternehmen verlassen, und die Arbeit des DSB von anderen Playern eingeschränkt wird, ist ein neues Verständnis der Arbeit sinnvoll. Das Event lieferte für diese Frage den Startschuss und eine erste Annäherung.

Über den Autor

Sebastian Himstedt
ist freier Journalist und Kommunikationsberater. Zuvor war er im Deutschen Bundestag und im eCommerce tätig. Seit einigen Jahren veröffentlicht er regelmäßig Beiträge zu Datenschutz und Digitalisierung in Fachpublikation.

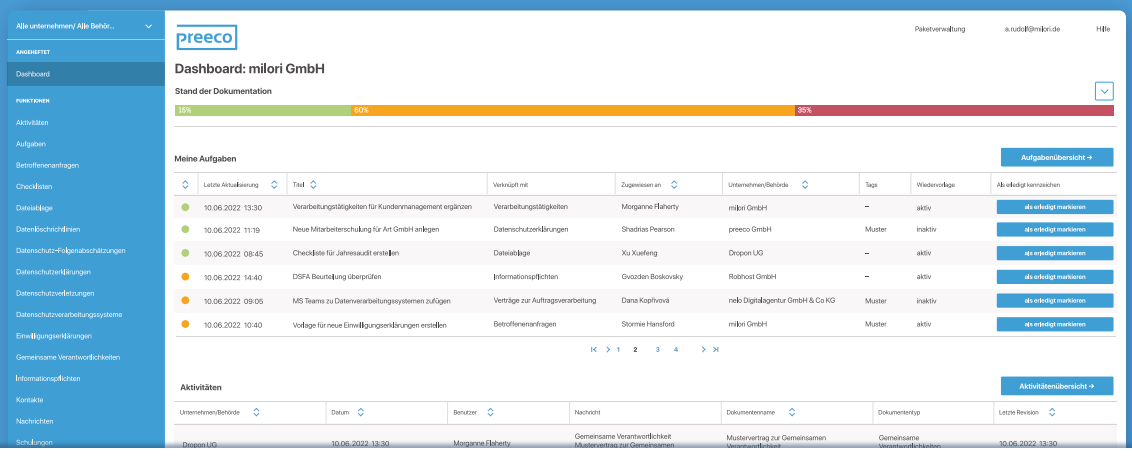
Anzeige

preeco

Die smarte Software für Datenschutzmanagement

Als interne und externe Datenschutzbeauftragte in Unternehmen oder Behörden werden Sie durch die Software **preeco | datenschutz und informationssicherheit** optimal unterstützt.

www.preeco.de/bvd



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

Jetzt neu: preeco | hinweisgeber – Ihr Tool zur Umsetzung der EU **Whistleblower-Richtlinie**

ADRESSHANDEL UND DIE OFFLINE-WERBUNG IN BRIEFKÄSTEN

Annelie Evermann, Giuliana Schreck

Unter Titeln wie „Datenschützer wollen Adresshandel untersagen" berichteten kürzlich mehrere Medien, dass die meisten Landesdatenschutzbeauftragten der Ansicht sind, dass die DS-GVO eine Weitergabe von Adressen für Marketingzwecke ohne Zustimmung der Betroffenen nicht mehr zulässt. Auch die Berliner Datenschutzbeauftragte vertritt diese Rechtsauffassung seit Inkrafttreten der DS-GVO und wendet sie in der eigenen Aufsichtspraxis an.

Adresshandel und die DS-GVO

Der Oberbegriff „Adresshandel" umfasst den Verkauf, die Vermietung und die sonstige Überlassung oder Nutzung im sogenannten Lettershop-Verfahren von Adressen und anderen personenbezogenen Daten zur Kontaktaufnahme. Die sogenannte Adressvermietung, also die einmalige Zurverfügungstellung von Adressdaten zu Werbezwecken, ist in der Praxis besonders verbreitet. Für werbende Unternehmen ist die Zusammenarbeit mit Adresshändlern vor allem im Rahmen der Neukundenakquise attraktiv.

Die Privilegierung nach alter Rechtslage (§§ 28, 29 BDSG a. F.) ist bekanntlich ersatzlos weggefallen. Die DS-GVO enthält keine ausdrückliche Regelung zur Zulässigkeit der Verarbeitung zum Zweck des Adresshandels, sodass sich die Zulässigkeit nach den allgemeinen Regelungen richtet. Die Frage der Rechtmäßigkeit der Datenverarbeitung stellt sich sowohl in Bezug auf die Adresshändler als auch in Bezug auf die werbenden Unternehmen und ist für jeden Verarbeitungsvorgang gesondert zu prüfen.[1]

Gemeinsame Verantwortlichkeit

Adresshändler und werbende Unternehmen sind für den zentralen Verarbeitungsvorgang der Nutzung personenbezogener Daten zur Versendung des Werbeschreibens (und damit zusammenhängend oft auch für die vorherige Selektion nach bestimmten Kriterien) in der Regel gemeinsam verantwortlich (Art. 26 Abs. 1 DS-GVO). Für die Stellung als Verantwortlicher kommt es nach der Rechtsprechung des Europäischen Gerichtshofs nicht auf eine Möglichkeit zum Zugriff auf die Daten an.[2] Maßgeblich ist, wer über die Zwecke und Mittel der Datenverarbeitung (mit-)entscheidet. Vorliegend sind beide Unternehmen an der Entscheidung über Zwecke und Mittel beteiligt: Das werbende Unternehmen veranlasst durch den entsprechenden Auftrag die Datenverarbeitung und gibt in der Regel – was jedoch für die Begründung der gemeinsamen Verantwortlichkeit nach der Rechtsprechung des EuGH nicht erforderlich ist – auch bestimmte Selektionskriterien vor. Der Adresshändler wählt die Adressen aus und stellt die Adressdaten zur Verfügung. Weder das werbende Unternehmen noch der Adresshändler können hinweggedacht werden, ohne dass der konkrete Datenverarbeitungsvorgang entfiele. Beide ver-

[1] Neben den werbenden Unternehmen und den Adresshändlern (spezialisierte Adressverlage, die über entsprechende Adressdatenbanken verfügen, sowie auch Unternehmen, die ihre Kundendaten vermieten) sind am Adresshandel auch Vermittler (sog. Listbroker) und andere Dienstleister beteiligt. Soweit diese personenbezogenen Daten verarbeiten, sind auch diese Verarbeitungsvorgänge unter Berücksichtigung der jeweiligen Rollen in jedem Einzelfall zu überprüfen, werden jedoch im vorliegenden Beitrag nicht behandelt.

[2] EuGH, Urteil vom 5. Juni 2018 – C-210/16, Rn. 38; Urteil vom 10. Juli 2018 – C-25/17 Rn. 68 f. Vgl. auch BlnBDI Jahresbericht 2019, S. 33 f. Bedeutung hat dies in der Praxis insbesondere auch deshalb, weil Betroffene ihre Rechte bei und gegenüber jedem einzelnen Verantwortlichen geltend machen können (Art. 26 Abs. 3 DS-GVO).

folgen einen gemeinsamen Zweck. Die Rechtmäßigkeit der Datenverarbeitung ist mithin von dem Adresshändler und von dem werbenden Unternehmen zu prüfen und nachzuweisen.

Rechtmäßigkeit der Verarbeitung

Als Rechtsgrundlage kommt neben einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO lediglich ein berechtigtes Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO in Betracht.

Einwilligung

Wirksame Einwilligungen sind in der Praxis kaum zu finden. Besonders häufig werden die Anforderungen an die Informiertheit der Einwilligung verkannt. Beim Einholen der Einwilligung muss ausdrücklich darauf hingewiesen werden, dass eine Verarbeitung zum Zwecke des Adresshandels erfolgt. Außerdem müssen die Unternehmen und die Produkte, für die geworben werden soll, konkret bezeichnet werden.[3] Dies stellt vielfach schon deshalb eine große Hürde dar, weil die Unternehmen und Produkte, für die künftig geworben werden soll, noch gar nicht bekannt sind.

Berechtigte Interessen

Äußerst praxisrelevant ist daher die Frage, inwieweit das berechtigte Interesse gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO als Rechtsgrundlage herangezogen werden kann.

Angesichts des weiten Begriffsverständnisses kann ein berechtigtes Interesse der Adresshändler an der wirtschaftlichen Verwertung personenbezogener Daten sowie der werbenden Unternehmen an der Werbung für ihre Produkte durchaus angenommen werden. Die Verarbeitung muss allerdings auch erforderlich sein und die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen dürfen nicht überwiegen. Die Frage, ob die Erforderlichkeit gegeben ist, darf an dieser Stelle nicht übersehen werden. Anders als der Begriff des berechtigten Interesses ist der Begriff der Erforderlichkeit eng auszulegen und vom Verantwortlichen ebenso wie das Vorliegen der übrigen Tatbestandsmerkmale nachzuweisen (Art. 5 Abs. 1 lit. a, Abs. 2 DS-GVO). So dürfte eine gezielte Ansprache einer bestimmten Zielgruppe u. a. durch die Wahl entsprechender zielgruppenspezifischer Medien, Orte und Veranstaltungen auch ohne Verarbeitung personenbezogener Daten möglich und zumutbar sein. Sofern dieser Aspekt nicht zur fehlenden Erforderlichkeit führt, ist er im Rahmen der Interessenabwägung zu berücksichtigen.

Interessenabwägung

Im Rahmen der Interessenabwägung wird oft Erwägungsgrund 47 Satz 7 der DS-GVO als Hauptargument für die Zulässigkeit von Werbung mittels Fremddaten und Adresshandel herangezogen. Dieser besagt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

Auch wenn der Adresshandel in der Praxis häufig mit dem Geschäftsfeld der Direktwerbung im Zusammenhang steht, verkennt diese Argumentation, dass Werbung und Adresshandel zwei unterschiedliche Verarbeitungszwecke darstellen, die keinesfalls in dem jeweils anderen enthalten sind.[4]

Zudem trifft Satz 7 nur eine Aussage zum berechtigten Interesse. Das Vorliegen berechtigter Interessen eröffnet jedoch erst die Möglichkeit einer Interessenabwägung ohne das Ergebnis dieser Abwägung vorwegzunehmen. Für die Interessenabwägung muss Erwägungsgrund 47 insgesamt in den Blick genommen werden, insbesondere die Sätze 1 bis 3. Es kommt damit maßgeblich auf die vernünftigen Erwartungen der betroffenen Person und die Beziehung zwischen der betroffenen Person und dem Verantwortlichen an. Neben den subjektiven Erwartungen der betroffenen Person im Einzelfall ist auch darauf abzustellen, was objektiv vernünftigerweise erwartet werden kann und insofern als sozialadäquat anzusehen ist.[5]

Teilweise wird vertreten, dass die vernünftigen Erwartungen der betroffenen Personen durch Transparenz beeinflusst oder erweitert werden könnten. Dies ist jedoch abzulehnen. Die Erwartungen der betroffenen Person können gerade nicht durch die nach der DS-GVO vorgesehenen Pflichtinformationen (Art. 13 bzw. Art. 14 DS-GVO) erweitert werden. Während die Nicht- oder Schlechterfüllung der Informationspflichten das Abwägungsergebnis aus Sicht des Verantwortlichen also negativ beeinflusst, hat die ordnungsgemäße Erfüllung der Informationspflichten keine Auswirkung auf die Abwägung.[6]

Es entspricht gerade nicht den allgemeinen Erwartungen einer Person, die zum Beispiel im Versandhandel etwas bestellt oder deren Daten zu anderen Zwecken in öffentlich zugänglichen Verzeichnissen oder in sozialen Netzwerken veröffent-

[3] BGH, Urt. v. 14.3.2017 – VI ZR 721/15, ZD 2017, 327 ff.

[4] Auch zur alten Rechtslage formulierte das OLG Frankfurt a. M., dass sich bereits aus § 28 Abs. 3 Satz 1 BDSG a. F. ergebe, „dass es sich hierbei um unterschiedliche Nutzungszwecke handelt und nicht etwa der Adresshandel als Unterfall der Werbung anzusehen ist", Urt. v. 24.1.2018, 13 U 165/16 = NJW 2018, 887, Rn. 37.

[5] Vgl. DSK-Orientierungshilfe Direktwerbung, S. 4.

[6] Vgl. DSK-Orientierungshilfe Direktwerbung, S. 4. Siehe auch EDSA, Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien, Version 2.0, vom 13. April 2021, Rn. 66.

licht sind, dass ihre Daten in der Folge dauerhaft gespeichert und einer beliebigen Anzahl an unbekannten Unternehmen für Werbezwecke zur Verfügung gestellt werden. Denn zu diesen Unternehmen stehen sie – anders als bei einem vorherigen Kundenverhältnis oder einer sonstigen Interessenbekundung – in keinerlei Beziehung. Die Nutzung des Lettershop-Verfahrens mag die Eingriffsintensität zwar zu einem gewissen Grad abschwächen, weil die Adressdaten auf diese Weise (außer bei Postrückläufern und Reaktionen) nicht an die werbenden Unternehmen weitergegeben werden. Unverändert ist aber auch bei dieser Konstellation, dass es üblicherweise nicht den vernünftigen Erwartungen der betroffenen Personen entspricht anlasslos von diversen unbekannten Unternehmen kontaktiert zu werden. Weder die Datenerfassung durch Adresshändler noch die weitere Verarbeitung durch diese oder das Versenden der Werbung selbst entsprechen den vernünftigen Erwartungen der betroffenen Personen, sodass die Interessenabwägung in der Regel zugunsten der betroffenen Person ausfällt. Das Fehlen einer entsprechenden Erwartungshaltung zeigt sich nicht zuletzt auch an den vielen bei den Datenschutzbehörden eingehenden Beschwerden in Bezug auf diese Werbepraxis. Allein die Tatsache, dass dieses Vorgehen gängige Werbepraxis ist, führt nicht dazu, dass es sozialadäquat ist.

Der Adresshandel greift zudem intensiv in das Recht auf Schutz der personenbezogenen Daten (Art. 8 GRCh) bzw. in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) ein. Teilweise wird argumentiert, dass die Regelung des Werbewiderspruchs in Art. 21 Abs. 2 und 3 DS-GVO zeige, dass der Gesetzgeber im Bereich der Direktwerbung von einer geringen Eingriffstiefe ausgegangen sei. Allerdings dürfte die Regelung des voraussetzungslosen Werbewiderspruchsrechts vielmehr zeigen, dass der europäische Gesetzgeber die erhebliche Belästigung durch Werbung erkannt hat und den Interessen der betroffenen Personen insoweit den Vorrang eingeräumt hat.

Mit dem Adresshandel ist ein Kontrollverlust über die eigenen personenbezogenen Daten verbunden. Bei Werbung fremder Unternehmen stellt die Erklärung des Widerspruchs – anders als bei der Bestandskundenwerbung – einen nicht unerheblichen Aufwand für die betroffenen Personen dar, ohne dass sie den Anlass für die Datenverarbeitung selbst gesetzt haben. Dies liegt auch an der großen Anzahl an Adresshändlern und Fremdadressen nutzenden Unternehmen. Es ist betroffenen Personen nicht zumutbar von jedem einzelnen Unternehmen die unerbetene Werbung durchlesen zu müssen, um – erfolgreich nur im Fall einer ordnungsgemäßen Belehrung – den Verantwortlichen zu identifizieren, um jeweils Widerspruch einzulegen. Zu beachten ist in diesem Zusammenhang auch, dass die präventive Eintragung in allgemeine Werbesperrlisten (sog. Robinsonlisten) gerade nicht allgemein wirksam ist, da ein Abgleich mit diesen Sperrlisten in Deutschland – anders als in anderen EU-Mitgliedstaaten – nur freiwillig ist und zudem der Kontrollverlust und die Risiken durch die massenhafte Datenverarbeitung, etwa bei Datenpannen, fortbestehen.

Schließlich ist zu berücksichtigen, dass ein entsprechendes Abwägungsergebnis nicht dazu führt, dass Unternehmen die zielgruppengenaue Neukundenakquise unmöglich gemacht wird. Allein die Tatsache, dass es sich bei der Datenverarbeitung ohne vorherige Einwilligung der Betroffenen möglicherweise um die einfachste oder wirtschaftlich sinnvollste Möglichkeit für die Verantwortlichen handelt, begründet allein noch nicht die Erforderlichkeit einer Datenverarbeitung und insbesondere nicht das Überwiegen der Interessen gegenüber den schutzwürdigen Interessen der betroffenen Personen.

FAZIT

Für den Handel mit Adressen und sonstigen personenbezogenen Daten zu Werbezwecken ist damit in der Regel anzunehmen, dass die schutzwürdigen Interessen der betroffenen Personen die Interessen des Adresshändlers und des Werbenden an der Verwertung der Adressen beziehungsweise der Produktwerbung überwiegen. Damit ist eine wirksame Einwilligung der betroffenen Personen erforderlich. Adresshändler und werbende Unternehmen müssen sich darauf einstellen, dass sie als (gemeinsam) Verantwortliche in die Pflicht genommen werden.

Dieser Artikel spiegelt die Meinung der Autorinnen wider und nicht zwangsläufig die der Berliner Beauftragten für Datenschutz und Informationsfreiheit.

Über die Autorinnen

Annelie Evermann
ist juristische Referentin bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Dr. Giuliana Schreck
ist juristische Referentin bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit

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

Datenschutzkonferenz 2022

Praxis | Recht | Innovation

» 25. - 27. September 2022 | Hotel Kö59 Düsseldorf

15 Stunden für Ihre Fortbildungsbescheinigung nach § 15 FAO

Es erwarten Sie u.a. diese Themen:

- Vor-Ort-Kontrolle – wenn die Aufsicht zweimal klingelt
- Umsetzung eines Löschkonzepts in der Praxis
- Die neuen EU-Standarddatenschutzklauseln – Best Practice
- Datenschutz-Compliance ohne Ressourcen
- Update Beschäftigtendatenschutz
- Wer zahlt den Deckel? – Erstattung und Versicherbarkeit von Bußgeldern
- Umgang mit Datenschutzverletzungen im Unternehmen
- Betroffenenrechte in der Praxis – Do's and Dont's
- Der Weg zu einem EuGH-Urteil im Datenschutzrecht
- TTDSG auf dem Radar – Wie prüft die Behörde?
- „Die 8 Fehler, die viele Unternehmen in 2022 beim Datenschutz machen – und wie man es besser machen könnte."

Freuen Sie sich auf neue Impulse durch:

Dr. Stefan Brink

Dr. Diana Ettig

Stephan Hansen-Oest

Dr. Nina Elisabeth Herbort

Stefanie Koch

Wiebke Reuter

Frederick Richter

David Sänger

Dr. Dominik Sorber

Jan Spittka

Malgorzata Steiner

Barbara Thiel

Dr. Paul Voigt

Tim Wybitul

Und vielen weiteren Referentinnen und Referenten.

Melden Sie sich jetzt an! **www.datenschutzkonferenz.de**

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

Medienpartner:

DATENSCHUTZ-BERATER

Kommunikation & Recht

Compliance Berater

DEEPFAKES MADE BY KI

Wie Künstliche Intelligenz Deepfakes ermöglicht und aufspüren hilft.

Nicolas Müller

In den letzten Jahren konnte durch Künstliche Intelligenz (KI) eine Vielzahl von Problemen gelöst werden, an denen herkömmliche Algorithmen bisher gescheitert waren. Ob für die automatisierte Übersetzung von Texten, für Assistenzfunktionen im Auto oder für die automatische Erkennung ungewöhnlicher Kontobewegungen, um Kreditkartenmissbrauch aufzudecken: KI entwickelt sich zu einem schlagkräftigen Werkzeug, welches in der Lage ist wiederholt auszuführende und für Menschen oft lästige Aufgaben effizient zu automatisieren. Somit hat KI das Potential unser aller Leben sicherer, angenehmer und besser zu gestalten.

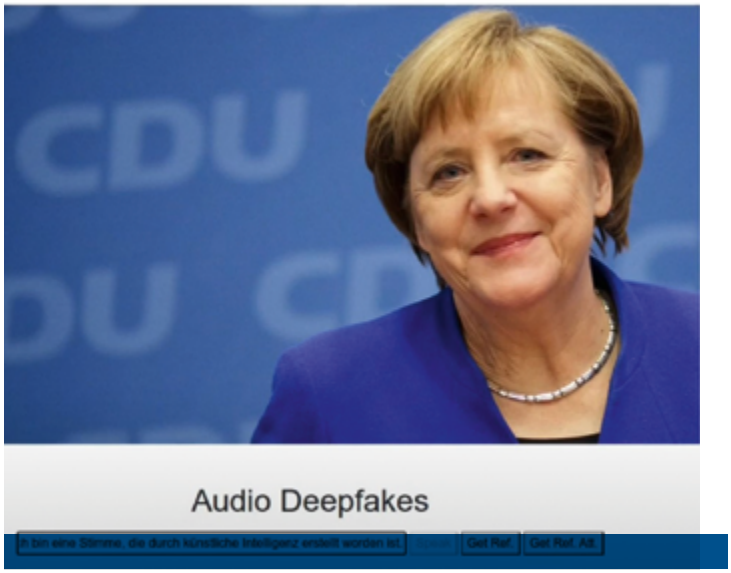
Wie viele andere Technologien kann KI allerdings auch missbraucht werden. Ein besonders eindrückliches Beispiel sind Deepfakes. Das sind durch KI erstellte Fälschungen von Audio- und Videoinhalten. In diesem Beitrag beschäftigen wir uns mit Deepfakes und fragen: Wie funktioniert diese Technologie? Wie verändert sie unsere Gesellschaft und wie können wir uns gegen die damit einhergehende Bedrohung wappnen?

Funktionsweise von Deepfakes

Wie werden Deepfakes beispielsweise von Audio- bzw. Videoinhalten von Personen mithilfe von KI erstellt? Zunächst benötigt die KI große Mengen an Trainingsmaterial, also in unserem Fall Ton- bzw. Videoaufzeichnungen, anhand welcher sie die charakteristischen Eigenschaften der Zielperson erlernt. Konkret bedeutet das beispielsweise Folgendes: Ein Angreifer möchte die Integrität einer bekannten Zielperson – beispielsweise Angela Merkel – verletzen, indem er ihr mittels Deepfake Worte in den Mund legt und sie Dinge tun lässt, die sie im echten Leben nie sagen oder tun würde. Hierzu benötigt er Trainingsdaten. Das können beispielsweise frei im Internet verfügbare Video- und Audioaufnahmen der Zielperson sein. Im Fall der ehemaligen Bundeskanzlerin Angela Merkel sind etwa diverse Reden, Ansprachen und Podcasts im Netz frei verfügbar. Ein Angreifer kann diese Daten herunterladen und der KI als Trainingsmaterial bereitstellen. Mithilfe dieser Daten lernt die KI, wie die Stimme von Angela Merkel klingt, wie ihr Gesicht aussieht und welche Mimik für sie typisch ist. Ähnlich wie Schauspieler*innen, die sich auf eine bestimmte Rolle vorbereiten, 'sieht' sich die KI die Trainingsdaten an und lernt aus diesen den Zusammenhang zwischen Text und Sprache bzw. Text und Lippenbewegung. Das funktioniert über die Technologie der sogenannten künstlichen, neuronalen Netze, die den Nervenbahnen des menschlichen Gehirns nachempfunden sind.

Das Ergebnis: Ein System, welches zu einem beliebigen Text, den man ihm gibt, automatisch eine Audio- oder Videosequenz erzeugt, in der der Text als gesprochenes Wort bzw. als Video wiedergegeben wird. Mit einer solchen Technik kann man sozusagen einen digitalen Klon der Zielperson – hier zum Beispiel der ehemaligen Bundeskanzlerin – erstellen, welcher vollkommen vom Angreifer kontrolliert wird. Dieser kann Frau Merkel nun buchstäblich jedes beliebige Wort in den Mund legen, wie folgendes Demovideo zeigt:[1]

[1] https://www.youtube.com/watch?v=VLo_xIAiKzU



Screenshot aus einem Deepfake-Erstellungstool mit Angela Merkel: Ein*e Angreifer*in gibt einen beliebigen Text ein (unten) und die KI erstellt die dazugehörige authentische Audiospur. So lassen sich der ehemaligen Bundeskanzlerin beliebige Worte in den Mund legen. [https://www.youtube.com/watch?v=MZTFoeAALmE]

Deepfakes als zweischneidiges Schwert

Was sind die Auswirkungen dieser Technologie auf uns und unsere Gesellschaft? Zunächst einmal ist offensichtlich, dass sich mit Deepfakes großer Schaden anrichten lässt: diffamierender Einsatz von Pornographie über gefälschte Gesichter in Videos, Betrug, Fake News, politische Verleumdung und Rufmord. In einem Fall wurde beispielsweise ein Buchhalter einer Firma durch einen Deepfake überlistet, der den Chef nachahmte und den Angestellten anwies Betrügern 200.000 US-Dollar ins Ausland zu überweisen[2]. Bekanntheit hat auch der Deepfake des ukrainischen Präsidenten Selenskyj erlangt. Hierin fordert ein gefälschter Selenskyj die ukrainische Armee zur Kapitulation auf.

Durch diese neue Bedrohung ändert sich auch, wie wir mit Medieninhalten umgehen: Sind durch Bildbearbeitungssoftware bereits Fotos als solche nicht mehr bedingungslos glaubwürdig, so verlieren durch Deepfakes jetzt auch bewegte Bilder und Tonspuren ihren unbedingten Anspruch auf Echtheit. Die konkreten Folgen für Gesellschaft, Politik und Justiz (zum Beispiel die Authentizität von Beweismitteln) lassen sich noch nicht absehen.

Das Aufkommen von Deepfakes macht ein Umdenken in der Art, wie wir mit persönlichen audio-visuellen Daten umgehen, unabdingbar: Jede von uns ins Internet gestellte Aufnahme, und sei es nur die Hochzeitsrede oder eine Ansprache auf der Abiturfeier, könnte nun unsere digitale Identität bedrohen. Der Demonstrator mit Angela Merkel zeigt: Es reichen bereits einige wenige Beispielaufnahmen von insgesamt rund 30 Minuten, um eine Person digital zu klonen.

Neue Chancen in unterschiedlichsten Bereichen

Doch Deepfakes eröffnen auch neue positive Anwendungsmöglichkeiten: Hier ist beispielsweise die Therapie von am Kehlkopf erkrankten Menschen zu nennen, bei der die Technologie Texte automatisiert in Audiosequenzen transformiert (sogenannte Text-to-Speech-Technologie) und so den Verlust der Stimme zumindest in gewissem Maße kompensieren kann. Denkbar ist, dass im Falle einer Krankheit die eigene Stimme mithilfe vorher angefertigter Aufnahmen rekonstruiert wird, wie etwa bei dem an ALS erkrankten Physiker Stephen Hawking. Weiterhin bietet die Synthese von Audio- und Videomaterial neue Möglichkeiten für die digitale Unterhaltungsbranche, beispielsweise wenn nicht gelungene Aufnahmen nach Drehschluss ohne persönliche Einbeziehung der Schauspieler*innen angepasst werden können.

Letztlich sind auch ambivalente Anwendungsfälle zu nennen, wie der Einsatz bei der Trauerbewältigung: Hier kann nach dem Tod eines geliebten Menschen ein entsprechender Deepfake erzeugt werden, der den Hinterbliebenen Mut, Trost und Optimismus schenkt. Ein prominenter Fall ist der Deepfake, den der US-amerikanische Rapper Kanye West seiner Ehefrau Kim Kardashian geschenkt hat: Darin wendet sich Kardashians mittlerweile verstorbener Vater an seine Tochter.[3]

Der Umgang mit bösartigen Deepfakes

Die Deepfake-Technologie lässt sich nicht per se verteufeln, sondern ist wie viele technologische Werkzeuge sowohl nutzbringend als auch schädlich einsetzbar. Wenn wir die Potentiale nutzbar machen wollen, gilt es den aktuellen Herausforderungen angemessen zu begegnen. Hier bieten sich vor allem drei Möglichkeiten an: Erstens die Sensibilisierung der Bevölkerung, um diese resilienter gegen die neue Bedrohung zu machen, zweitens algorithmische Lösungen, um gefälschte Inhalte schnell, zuverlässig, effizient und automatisiert erkennen zu können, und drittens Signaturverfahren, um echte Inhalte unzweifelhaft als vertrauenswürdig zu markieren.

Sensibilisierung der Konsument*innen von Medieninhalten

Ein wesentlicher Schritt bei der Sensibilisierung von Menschen bezüglich Deepfakes ist diesen die Möglichkeiten der Technologie vor Augen zu führen und sie dadurch zu motivieren Medieninhalte kritisch zu hinterfragen. Wer einmal

[2] https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/?sh=3102804224l6

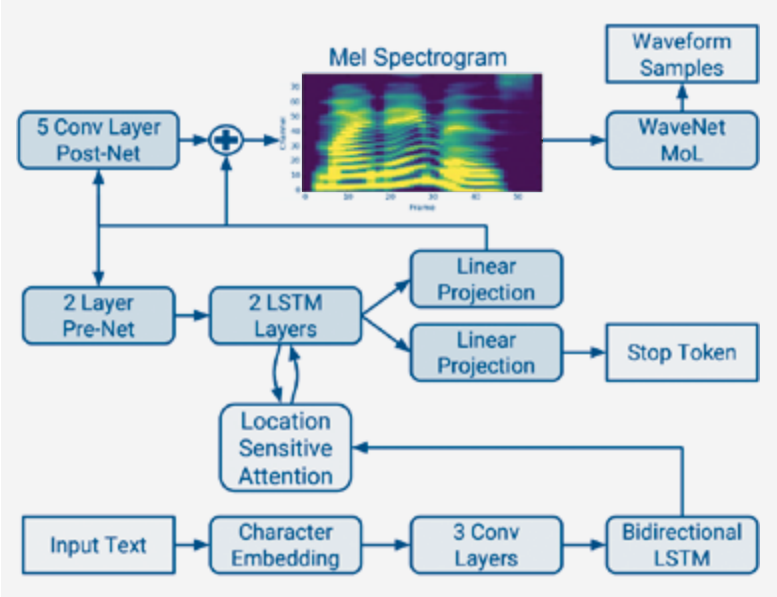
[3] https://www.themodems.com/lifestyle/kanye-west-gave-kim-kardashian-a-hologram-of-her-father-for-her-birthday#:~:text=The%20Deepfake%20hologram%20used%20AI,at%20the%20age%20of%2059.

eine gefälschte Angela Merkel gesehen hat, ist auch bei anderen Medieninhalten von ihr kritisch und hinterfragt deren Authentizität. Eine effektive Strategie bei der Überprüfung der Echtheit von Mediendaten ist der Abgleich verschiedener, möglichst vertrauenswürdiger Quellen.

Um ein Bewusstsein für das Missbrauchspotential von Deepfakes zu schaffen, entwickelt das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC entsprechende Demonstratoren. Eine kürzlich von uns durchgeführte Nutzerstudie[4] hat ergeben, dass schon eine kurze Auseinandersetzung der Nutzer*innen mit Audio-Deepfakes die Erkennungsrate von Fälschungen bei diesen Nutzer*innen deutlich steigert. Dies kann online bei einem Spiel ausprobiert werden: Hier werden den Nutzer*innen Audioaufnahmen vorgespielt, die entweder echt oder gefälscht sind. Die Spieler*innen haben die Aufgabe diese zu klassifizieren und bekommen im Anschluss das richtige Ergebnis mitgeteilt[5]. Schon nach kurzer Zeit (20 vorgeführte Aufnahmen reichen aus) lernt unser Ohr Fälschungen und Originale besser zu unterscheiden und die Erkennungsrate von Audio-Deepfakes steigt von 66 auf 80 Prozent.

Automatisierte Erkennung von Fälschungen

Neben der Sensibilisierung ist es grundlegend gefälschte Medieninhalte automatisiert als solche zu erkennen: Hier geht es darum Audio- und Videomaterial automatisch auf Echtheit zu überprüfen. Vorstellbar ist beispielsweise, dass das auf Social-Media-Plattformen veröffentlichte Material nur nach einer erfolgreichen Echtheitsprüfung geteilt werden kann. Ein System, welches Deepfakes sicher und verlässlich erkennt, würde die Verbreitung von Falschinformationen effektiv unterbinden. Wie muss ein solches System aufgebaut sein? Klar ist, dass hier ebenfalls KI zum Einsatz kommen muss, denn die Echtheit von Medieninhalten lässt sich nicht auf herkömmliche Art algorithmisch erschließen. Wir benötigen also eine zweite Künstliche Intelligenz, welche lernt, wie Deepfakes aussehen und welche (für den Menschen gegebenenfalls nicht wahrnehmbaren) Eigenschaften sie aufweisen. Derartige Systeme werden mit großen Datensätzen an originalen, unverfälschten Medieninhalten trainiert und sind dann in der Lage, unbekannte Deepfakes zu erkennen, so dass diese direkt gelöscht werden könnten.



Die Architektur eines neuronalen Netzwerks, welches Deepfakes erstellt. (https://pytorch.org/hub/nvidia_deeplearningexamples_tacotron2/). Unten links beginnt die Verarbeitung des Inputs, der in diesem Fall der transkribierte Text ist. Durch eine Sequenz von neuronalen Layern wird dieser Input aufgearbeitet und transformiert. Schließlich erzeugt das Netzwerk die Ausgabe (Waveform Samples, oben rechts): Audioaufnahmen der Zielpersonen, passend zum entsprechenden Input-Text.

Es gibt bereits große, internationale Wettbewerbe, bei denen Softwareentwickler*innen ihre verschiedenen Erkennungssysteme gegeneinander antreten lassen[6,7]. Die Entwicklung der Technik ist bei der Erkennung von Fälschungen allerdings noch nicht so weit fortgeschritten wie bei der Erstellung von Deepfakes. Der Grund ist, dass Erkennungsmethoden der Erstellung immer hinterherlaufen, da sie auf entsprechende Trainingsdaten angewiesen sind. Die Erkennung von neuen, unbekannten Deepfakes bleibt also eine der aktuellen Herausforderungen.

Signaturverfahren

Die beiden bereits beschriebenen Lösungsansätze basieren grundlegend darauf gefälschten Medieninhalten entgegenzutreten und diese entweder zu erkennen oder zumindest ihre Wirksamkeit einzuschränken. Alternativ dazu kann man auch die Vertrauenswürdigkeit von Original-Material stärken:

[4] https://arxiv.org/pdf/2107.09667.pdf
[5] https://Deepfake-demo.aisec.fraunhofer.de/
[6] https://www.asvspoof.org/
[7] https://ai.facebook.com/blog/Deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/
[a] https://thispersondoesnotexist.com/
[b] http://this-voice-does-not-exist.com/

Hierzu bieten sich signaturbasierte Verfahren an, wie wir sie schon aus dem World-Wide-Web oder im Zusammenhang mit signierten E-Mails kennen.

Echte Inhalte (wie Nachrichten oder Websites) werden hier von einer vertrauenswürdigen Stelle als 'echt' markiert. Dies geschieht durch die Erstellung einer elektronischen Signatur mittels spezieller, breit im Einsatz befindlicher Verschlüsselungstechnologie. Jeder potenzielle Emfpänger kann die Echtheit der Signatur prüfen. Dafür wird ein digitales Zertifikat benötigt, das frei auf öffentlichen Servern zur Verfügung gestellt werden kann. Beispielsweise kann eine E-Mail so signiert werden, dass durch eine Veränderung des Mailinhalts die Signatur ungültig wird. Das Mailprogramm zeigt dem Empfänger der E-Mail an, dass die Signatur ungültig ist, wenn eine Veränderung vorgenommen wurde, sodass beim Lesen der Mail festgestellt werden kann, ob diese manipuliert worden ist oder nicht. Dieses Verfahren ist auch für Medienhalte, also für Video- und Audioaufnahmen denkbar. Hierzu müsste das beispielsweise auf dem Smartphone aufgenommene Video direkt auf dem Gerät signiert werden und die Software, mit der Videos und Audios abgespielt werden, müsste analog zum E-Mail-Programm die Signatur prüfen und Nutzer*innen informieren. Die Herausforderung hierbei ist allerdings, wie wir mit Material umgehen, welches keine oder eine ungültige Signatur hat. Ist dieses dann automatisch ein Fake?

Die verwackelten und schlecht auflösenden Videoclips, die wir zurzeit aus der Ukraine zu sehen bekommen, zeigen: Es gibt eine große Heterogenität an Aufnahmegeräten, und die für die Umsetzung von Signaturverfahren und deren automatischer Prüfung benötigte Software kann gegebenenfalls (noch) nicht überall vorausgesetzt werden.

FAZIT

Künstliche Intelligenz verändert unser Leben, und das gilt besonders für unsere digitale Identität. Deepfakes bedrohen die Authentizität von Medieninhalten und erfordern geeignete Gegenmaßnahmen. Denn obwohl die Technologie für gutartige Zwecke genutzt werden kann, ist das Missbrauchspotenzial enorm. Die automatisierte Erkennung von Deepfakes sowie die Sensibilisierung der Menschen und die Stärkung ihrer Medienkompetenz muss deshalb im Vordergrund stehen. Und nicht zuletzt müssen wir uns bewusst sein, dass wir Angreifer*innen die Möglichkeit geben Deepfakes von uns zu erstellen, wenn wir eigene Audio- und Videoaufnahmen veröffentlichen oder deren Anfertigung zustimmen (wie etwa über die Diktatsoftware des Android-Betriebssystems). Derartige persönliche Daten sind durch das Aufkommen von Deepfakes nun noch schützenswerter geworden.

Über den Autor

Nicolas Müller
arbeitet seit 2017 am Fraunhofer AISEC als wissenschaftlicher Mitarbeiter in der Abteilung „Cognitive Security Technologies". Seine Forschungsschwerpunkte liegen im Bereich Deep-Learning, Text-to-Speech Synthesis mit Bezug auf Audio-Deepfakes und Adversarial Machine Learning. Er hat ein Studium in Mathematik und Informatik an der Universität Freiburg abgeschlossen.

▶ www.aisec.fraunhofer.de

Anzeige

- Interne & externe Datenschutzbeauftragte -
Sie suchen eine Haftpflicht-Versicherung? Sie möchten Ihre bestehende Police vergleichen?

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

Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.
- exklusives Wording (eDSB und erweiterte Tätigkeiten im Datenschutz mitversichert)
- optional inkl. Unternehmensberater, Informationssicherheits-Beauftragter
- niedrige Prämien & professionelle Beratung

+++ Neu +++
- Leistungs-Update
- Jahreshöchstleistung: das 4-fache der Versicherungssumme

Für nähere Informationen rufen Sie uns gerne an: 06174 - 96843-0 oder unter www.bvdnet.de (Mitgliederbereich)

Butz - Versicherungsmakler GmbH Ansprechpartner: Herr Jared Butz Tel: 06174 - 96843-0 Fax: 06174 - 96843-29
info@butz-versicherungsmakler.de www.butz-versicherungsmakler.de

STEPHAN REHFELD, PATRICK GRIHN, JOACHIM RIES

DATENSCHUTZAUDITS UND VERHALTENSREGELN

Wie ist der aktuelle Stand?

Einleitung

Menschen lieben Zertifikate, Medaillen und Urkunden. Im geschäftlichen Bereich werden Webseiten und auch Briefpapier mit Siegeln geschmückt, um den Empfänger zu beeindrucken oder von anderen Attributen zu überzeugen. Doch haben solche Siegel ein sehr unterschiedliches Gewicht und häufig ist dem Siegel-Adressaten die Aussage eines Siegels nicht bekannt. Für Unternehmen ist die Durchführung eines Datenschutzaudits eine Investition, an die konkrete wirtschaftliche Erwartungen geknüpft sind. Unternehmen hoffen durch Datenschutzaudits Vertrauen beim Kunden oder Auftraggeber zu schaffen und somit beispielsweise einen Vertragsabschluss zu erleichtern. Dies kann aber nur mit anerkannten Siegeln und standardisierten Zertifizierungsverfahren erreicht werden. Wie steht es also um Datenschutzzertifikate und die Anerkennung von Datenschutzsiegeln in der Wirtschaft?

Geschichte des Datenschutzaudits

Gesetzlich geregelte Datenschutzaudits – § 9a BDSG 2001

Im Datenschutz wurde das Konzept der Datenschutzzertifizierung das erste mal im Bundesdatenschutzgesetz (BDSG) im § 9a BDSG 2001 erwähnt. Um den § 9a BDSG 2001 mit Leben zu füllen, hätte es eines Datenschutzauditgesetzes (DSAG) bedurft. Das Datenschutzauditgesetz hat es aber nie über das Entwurfsstadium hinaus geschafft.[1] Anders war dies auf Landesebene. In Schleswig-Holstein gab es im Landesrecht die Möglichkeit für Behörden des Bundeslandes sich durch das ULD freiwillig auditieren zu lassen. Auch gab es in Schleswig-Holstein ein Datenschutz-Gütesiegel für Produkte.Die DSGVO sieht in Art. 42 ebenfalls Datenschutzaudits vor. So konnte die Wirtschaft seit Veröffentlichung des Verordnungstextes in 2016 hoffen, dass es doch noch dazu kommt, dass es ein gesetzlich anerkanntes Auditverfahren geben wird. Die Aufsichtsbehörden haben angekündigt, dass 2022 das Jahr sein wird, in dem nach 21 Jahren Wartezeit nun endlich die ersten Organisationen ein gesetzliches Datenschutzauditverfahren durchlaufen werden.

Privatwirtschaftliche Anstrengungen um ein Datenschutzaudit

In der ISO (International Standardization Organisation) wurde ab ca. 2011 daran gearbeitet ein weltweit einsetzbares Datenschutzmanagementsystem zu normieren. Dies kann dann die Grundlagen für eine international anerkannte Datenschutzzertifizierung sein. Vorbild war das Informationssicherheitsmanagementsystem (ISMS) der ISO 27001, dessen Zertifizierung ein großer Erfolg ist und weltweit Anerkennung findet.

Für ein weltweit gültiges Datenschutzmanagementsystem ist die Grundlage das Privacy Framework der ISO 29100, dass auf den international anerkannten Datenschutzprinzipien des „OECD Privacy Framework“[2] basiert und weltweit einen Benchmark für eine Baseline-Privacy schafft. 2016 wurde mit der Arbeit an dem Privacy Information Management System (PIMS) begonnen, was 2019 in der ISO 27701 veröffentlicht worden ist.

Organisation von Audits, Zertifikaten und Siegeln

Privatwirtschaftlich geregelte Siegel

Die meisten Audits und auch Siegel sind privatwirtschaftlich organisiert. Das am meisten verbreitete und demnach auch bekannteste Siegel ist ein ISO 9001-Zertifikat zum Qualitätsmanagement. In solchen Fällen organisiert sich die Wirtschaft selbst. DIN- und ISO-Normen sind als Maßstab in Deutschland am verbreitesten.

Gesetzlich geregelte Siegel auf Basis von Audits und Verhaltensregeln

In seltenen Fällen regelt der Gesetzgeber ein Zertifizierungsverfahren. In Art. 42 DSGVO hat der europäische Gesetzgeber die Durchführung von freiwilligen Datenschutzaudits ermöglicht und Anforderungen formuliert.

Zusätzlich hat der europäische Gesetzgeber in Art. 40 DSGVO das Mittel der genehmigten Verhaltensregeln eingeführt.

[1] https://dserver.bundestag.de/btd/16/120/1612011.pdf

[2] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Das Deutsche Institut für Normung (DIN) e.V. hat seinen Sitz in Berlin. Als privatwirtschaftlich organisierter Projektmanager steuert das DIN Normungsprozesse. Foto: Nadja Bunk.

Unterschied zwischen einer Zertifizierung und genehmigten Verhaltensregeln

Die DSGVO unterscheidet zwischen Zertifizierungen und genehmigten Verhaltensregeln (Code of Conduct, CoC). Zweck einer Zertifizierung nach Artikel 42 DSGVO ist „nachzuweisen, dass [die DSGVO] bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird." Verantwortliche weisen also gegenüber den Zertifizierungsstellen die Konformität mit der DSGVO nach. Zertifizierungsstellen können die Datenschutz-Aufsichtsbehörden oder akkreditierte Zertifizierer sein.

Verhaltensregeln nach Artikel 40 DSGVO sind Konkretisierungen einzelner Aspekte der DSGVO. Verhaltensregeln werden durch Verbände oder andere Vereinigungen ausgearbeitet, geändert oder erweitert. Verantwortliche oder Auftragsverarbeiter können dann den Verhaltensregeln beitreten. Die Einhaltung der Verhaltensregeln wird durch eine akkreditierte Stelle überwacht.

In beiden Fällen können Verantwortliche oder Auftragsverarbeiter nachweisen, dass sie entweder Anforderungen erfüllen oder sich dazu selbstverpflichtet haben gewisse Anforderungen zu erfüllen, die über die gesetzlichen Anforderungen hinausgehen. Auch im Falle der Selbstverpflichtung gibt es einen Überwachungsmechanismus.

In beiden Fällen wird dies durch ein Siegel gegenüber Dritten kommuniziert.

Konzepte

Kurzbeschreibung zur Artikel-42-Zertifizierung

Mit dem Wirksamwerden der DSGVO zum 25.05.2028 soll eine Art. 42-Zertifizierung nach ErwGr 100 die Einhaltung des Datenschutzrechts verbessern sowie einen raschen Überblick über das Datenschutzniveau von Prozessen und Dienstleistungen in einem Unternehmen/einer Organisation gewährleisten. Die Grundlage für die Prozessauditierung orientiert sich an der DIN EN ISO 17065 und EN ISO 17067 sowie an ergänzenden Anforderungen – daraus leitet sich ab, dass der Prüfgegenstand einer Art. 42-Zertifizierung kein Datenschutzmanagment-System ist. Die deutschen Aufsichtsbehörden (DSK) nutzen die Art. 42-Zertifizierungen zur „Marktbereinigung", da die Zertifizierungen nach dem BDSG-alt nicht mehr auf den neuen Rechtsstand ab dem 25.05.2018 überführt werden durften – es soll eine Vereinheitlichung der Prüfstandards geben. Aufgrund der DSGVO als Prüfgegenstand ist die Ausrichtung des Zertifikats auf die Staaten der EU gegeben – eine darüber hinausgehende, internationale Wirkung ist damit nicht verbunden. Die Anforderungen an die Zertifzierer sind sehr hoch. Die Akkreditierung durchläuft sechs Phasen und fordert von den Zertifizierungsstellen spätestens alle fünf Jahre die Beantragung eines Reakkreditierungsverfahrens. Bis zum Stand März 2022 wurde von elf Akkreditierungsanträgen ein Programm von der DAkkS und den Aufsichtsbehörden genehmigt und zur weiteren Beurteilung an die Europäische Datenschutzaufsichtsbehörde (EDSA) weitergeleitet.

Kurzbeschreibung ISO/IEC 27701

Die ISO 27701 ist eine Erweiterung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 um den Datenschutz. Wie alle großen Managementsysteme der Internationalen Standardisierungsorganisation (ISO) basiert das Datenschutz-Manage-

PRIVACYSOFT
Datenschutzmanagement as a Service

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

Vorlagen
Datenschutzdokumentation
Checklisten
E-Learning
Auditmodul
Mehrsprachig

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

mentsystem auf der High Level Structure (HLS), in der alle relevanten Mechanismen eines Managementsystems beschrieben sind. Das DIN hat die ISO 27701 in den deutschen Normenkanon übernommen. Die Anforderungen aus der ISO 27701 sind zertifizierungsfähig. Als Ergänzungsnorm zur ISO 27001 kann eine erfolgreiche Zertifizierung der Norm nur erfolgen, wenn die Organisation erfolgreich nach ISO 27001 zertifiziert ist. Ein Zertifikat nach ISO 27701 sagt aus, dass die Organisationen ein Datenschutz-Managementsystem (DSMS) nach ISO 27701 erfolgreich betreibt. Da die ISO 27701 international ausgerichtet ist, kann die DSGVO ein Datenschutzgesetz neben anderen sein, welches als Anforderung im PIMS beachtet wird.

Kurzbeschreibung VdS 10010

Die VdS 10010 wurde ab 2017 von einem Expertenteam der VdS Schadenverhütung GmbH entwickelt und liegt seit Dezember 2017 vor. In den Richtlinien werden Datenschutzprozesse, Datenschutzanforderungen nach DSGVO und eine Mindestdokumentation beschrieben. Bei der VdS 10010 ist eine hohe Affinität zu dem Managementsystem der ISO 27001 erkennbar.

BEISPIEL ZERTIFIZIERUNG VON ISO- UND DIN-NORMEN

ISO-Normen werden weltweit nach dem Konsenzprinzip erstellt und weiterentwickelt. In den nationalen Normungsinstitutionen arbeiten Experten an der fachlichen Entwicklung einer Norm. Die Ergebnisse dieser Facharbeit werden dann auf internationaler Ebene diskutiert und abgestimmt. Ergebnis dieses meist mehrjährigen Prozesses ist die offizielle Veröffentlichung eines neuen Standes einer Norm. Möchte sich eine Organisation zertifizieren lassen, so wird die Konformität oder Nicht-Konformität der Organisation mit einer oder mehrerer Normen regelmäßig durch einen anerkannten Zertifizierer durchgeführt. Dabei muss sich der Zertifizierer selbst Regeln unterwerfen und auch das Zertifizierungsverfahren ist reglementiert. Der Zertifizierer wird durch eine offizielle nationale Akkreditierungsstelle (in Deutschland DAkkS) überwacht. Ein Siegel, dass von einem nicht anerkannten Zertifizierer ausgestellt worden ist, hat einen geringeren Stellenwert als ein Siegel eines anerkannten Zertifizierers und wird im Wirtschaftsverkehr als Nachweis häufig nicht akzeptiert. Auch verhält es sich so mit Siegeln, die nicht auf ISO- oder DIN-Normen beruhen.

Die VdS 10010 beschreibt bewusst ein leichtgewichtiges DSMS, damit auch KMU in der Lage sind die Anforderungen an eine erfolgreiche Zertifizierung zu erfüllen. Durch die Kompatibilität zu einem ISMS nach ISO 27001 ist ein späterer Umstieg von Organisationen auf die ISO 27701 möglich. Kritik an Zertifikaten nach VdS 10010 ist, dass die VdS gleichzeitig die Auditoren stellt und die Auditberichte prüft und freigibt. Das mehrstufige System von Akkreditierer, Zertifizierer und Auditor wird bei diesen Zertifikaten nicht eingehalten.

Aussage eines Siegels zu den unterschiedlichen Zertifizierungskonzepten

Ein Siegel zur ISO/IEC 27701 oder zur VdS 10010 sagt lediglich aus, dass die zertifizierte Organisation ein Datenschutzmanagementsystem konform nach der jeweiligen Norm betreibt. Es wird aber nicht die Aussage getroffen, dass die Organisation zu dem Zeitpunkt des Audits DSGVO-konform war. Anders ist dies bei einer Artikel-42-Zertifizierung. Hier beschreibt der Gesetzgeber den Zweck der Datenschutzzertifizierung: „[…] Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingehalten wird." (Art. 42 Abs. 1 Satz 1 DSGVO).

Verhaltensregeln (Code of Conduct)

Erst vor kurzem wurde vom BfDI die Verhaltensregeln für Notare verabschiedet.[3] Der BfDI führt dazu selber aus „Notarinnen und Notare erhalten konkrete Orientierung in Datenschutzfragen. Gleichzeitig gewährleisten die Verhaltensregeln den Bürgerinnen und Bürgern ein verbindliches, einheitliches und hohes Sicherheitsniveau."[4] Der BfDI unterstreicht seine Hoffnung, dass zukünftig das Mittel der Verhaltensregeln zur Verbesserung des Datenschutzes genutzt wird. In Deutschland wird momentan an der Genehmigung weiterer Verhaltensregeln gearbeitet, z.B. dem Projekt „Trusted Data Processor".

Kurzbeschreibung „Anforderungen an Auftragsverarbeiter nach Art. 28 DSGVO"

„Trusted Data Processor" konkretisiert und standardisiert das Zusammenwirken von Auftraggeber und Auftragnehmer im Bereich der Auftragsvergabe beim Abschluss eines Auftragsverarbeitungsvertrages und gibt Auftragsverarbeitern eine Möglichkeit ihre Zuverlässigkeit gegenüber den Auftraggebern vereinfacht durch Beitritt zu dieser Verhaltensregel nachzuweisen. Durch die damit einhergehende Markttransparenz und stärkere

[3] https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2022/07_Verhaltensregeln-Notare.html;jsessionid=7DED9F469DFD438B495AFD9D00D617A0.intranet241?nn=252136

[4] ebd.

Verpflichtung zur Eigenkontrolle des Auftragsverarbeiters profitieren zum einen die beteiligten Unternehmen durch ein nachweisbares Management des Datenschutzes bei Auftragsverarbeitungsverhältnissen. Zum anderen profitieren Betroffene durch transparente sowie einheitliche Standards bei der Auftragsverarbeitung, was ihr Vertrauen in die datenverarbeitenden Stellen stärkt. Im CoC werden zum Beispiel Geschäftsprozesse zur Auditierung von Subauftragnehmern oder auch zur Meldung von Datenschutzvorfällen vorgegeben. Keine Aussage wird zum Vertragstext oder der Beschreibung der technischen und organisatorischen Maßnahmen getroffen. Erarbeitet wurde der CoC durch den BvD und die GDD. Der CoC ist eine Fortentwicklung der Verhaltensregel DS-BvD-GDD-01. Sogenannter Code Owner ist der Verein zur Förderung von Verhaltensregeln (VFV). Die praktische Betreuung und Überwachung der Einhaltung des CoC wird von der DSZ GmbH geleistet. Der CoC ist ein nationaler Standard und auf Anwender in Deutschland beschränkt. Eine Akzeptanz als europäischer Standard wird durchaus angestrebt.

Erfolgsfaktoren für Datenschutzsiegel und Verhaltensregeln

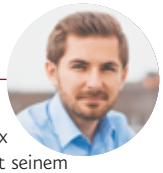
Anfang 2022 hat der BvD eine Befragung seiner Mitglieder zu Datenschutzaudits und Verhaltensregeln durchgeführt. Anhand der Ergebnisse der Befragung lassen sich Erfolgsfaktoren für eine Datenschutzzertifizierung ableiten. An den Zahlen lässt sich ablesen, dass es in der Wirtschaft durchaus ein Interesse an Datenschutzsiegeln gibt. Rund 37 Prozent der Befragten interessierten sich für eine Artikel-42-Zertifizierung, circa 30 Prozent für eine ISO 27701-Zertifizierung und etwa 20 Prozent interessierten sich für den CoC „Trusted Data Processor“. 64 Prozent der Befragten würden ein Siegel bis 2024 anstreben. 70 Prozent sind der Meinung, dass die Vorbereitung eines Datenschutzaudits oder der Beitritt zum CoC durch einen externen Berater begleitet werden muss und 75 Prozent sind die Kosten für ein Auditierung oder den Beitritt zu Verhaltensregeln nicht bekannt. Ungefähr die Hälfte der Befragten konnten sich für Datenschutzaudits oder dem Beitritt zum CoC ein Budget von bis zu 6.000 Euro vorstellen. Ab Kosten von mehr als 10.000 Euro brach das Interesse an Datenschutzaudits und CoCs massiv ein.

Fazit der Befragung

Erstaunlicherweise sind die Befragten indifferent, ob ein Datenschutzsiegel gesetzlich organisiert sein muss oder privatwirtschaftlich organisiert sein kann. Auch besteht eine hohe Bereitschaft die eigenen Datenschutzprozesse an die Anforderungen anzupassen und dabei auch auf externe Hilfe zurückzugreifen. Allerdings wird ein Datenschutzsiegel als Investition bewertet und Unternehmen haben sich anscheinend klare Budgetgrenzen gesetzt.

Über die Autoren

Dipl.-Ök. Stephan Rehfeld
ist externer Datenschutzbeauftragter der scope & focus GmbH Hannover und akkreditierter Datenschutzauditor der DQS GmbH. Er ist BvD-Vorstandsmitglied und Mitglied im Ausschuss Prüfaufgaben Datenschutzbeauftragter des BvD. Ferner ist er in der GDD, der Bitkom und in der Fachgruppe Datenschutz von Niedersachsen engagiert. Als stimmberechtigtes Mitglied des AK05 des NIA27 des DIN arbeitet er außerdem aktiv an der Erstellung und Überarbeitung von Datenschutz-ISO- und -DIN-Normen mit.



Patrick Grihn
ist Geschäftsführer der nextindex GmbH & Co. KG und betreut mit seinem Team KMUs in den Bereichen IT-Infrastruktur, IT-Sicherheit und Datenschutz.

Joachim Ries M.A., LL.M.
arbeitet als Datenschutzkoordinator und Leiter der Datentreuhandstelle am Universitätsklinikum Augsburg und beschäftigt sich mit dem Datenschutz in der klinischen Versorgung sowie der medizinischen Forschung.

PRIVACYSOFT
Datenschutzmanagement as a Service

ENTSCHEIDEND IST DAS WISSEN FÜR MORGEN.

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

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

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

DATENSCHUTZ IM VEREIN

Viele offene Fragen für ehrenamtlich Engagierte.

Hendrik vom Lehn

Gemäß den Erhebungen des Freiwilligensurvey engagieren sich in Deutschland knapp 30 Millionen Menschen freiwillig.[1] Dieses Engagement findet in etwa 600.000 eingetragenen Vereinen, aber auch in Organisationen und Gruppierungen anderer Rechtsnatur, statt. Für sie alle gilt die Datenschutzgrundverordnung (DSGVO), denn die Grenzen der Haushaltsausnahme sind sehr eng gesteckt und gemeinschaftsbezogenes Engagement verlässt per Definition diesen Bereich. Daher stellt sich die Frage, an welchen Stellen Engagierte Informationen zur DSGVO finden und von welchen Stellen sie hierbei unterstützt werden.

Hilfestellung zur DSGVO-Umsetzung erhalten Vereine und ehrenamtlich Engagierte vor allem aus den vorhandenen Strukturen ihres jeweiligen Bereichs. Viele Verbände waren zum Anwendungsbeginn der DSGVO in 2018 aktiv und bemühen sich Materialien für die durch sie vertretenen Mitgliedsorganisationen zur Verfügung zu stellen. Dies reicht von einfachen Linksammlungen bis hin zu umfangreichen Paketen mit Handlungsleitfäden und Vorlagen. Besonders die Sportverbände waren und sind hier recht aktiv. Es gibt jedoch auch Verbände, die nur auf allgemeine Informationen verweisen oder gar keine Informationen zur DSGVO bereithalten.

Da längst nicht alle Vereine und Gruppierungen in Form von Verbänden organisiert sind, ist es wichtig, dass es zusätzlich zu diesen Angeboten auch allgemeine Informationen zur DSGVO gibt. In diesem Bereich sind die Datenschutzaufsichtsbehörden der Länder aktiv geworden, denen die Aufsicht über Vereine als nichtöffentliche Stellen obliegt. Bei immerhin zwölf der 16 Aufsichtsbehörden gibt es spezifische Informationen zum Datenschutz im Verein. Diese Handreichungen sind in den meisten Fällen jedoch sehr abstrakt gehalten und gehen an manchen Stellen kaum über den Gesetzeswortlaut hinaus.

Daneben gibt es noch weitere Akteure, die Engagierten Datenschutzwissen als eines von mehreren Themen vermitteln. So zum Beispiel Deutschland sicher im Netz e.V. mit seinem Angebot „Digitale Nachbarschaft“[2] oder die *Deutsche Stiftung für Engagement und Ehrenamt* mit ihrer Webinarreihe #DSEEerklärt.[3] Zudem findet man einige Angebote kommerzieller Anbieter, die Informationen zu rechtlichen Themen im Vereinskontext anbieten. Datenschutz ist bei diesen Angeboten jedoch nur ein Bestandteil und den datenschutzspezifischen Informationen fehlt an vielen Stellen die notwendige Tiefe.

Die *Stiftung Datenschutz* ergänzt diese Möglichkeiten seit kurzem mit ihrem Angebot „Datenschutz im Ehrenamt“[4] (siehe Info-Box). Hier versuchen wir die aus unserer Sicht notwendige, inhaltliche Tiefe mit einer praxisnahen Darstellung der Inhalte zu verbinden. Bei vielen Fragestellungen ist jedoch eine Einzelfallbetrachtung notwendig, so dass auch wir an manchen Stellen um abstrakt gehaltene Betrachtungen nicht umhinkönnen. Ein gewisses Maß an Einarbeitung von Seiten der Vereine und engagierter Personen ist also notwendig.

[1] https://www.bmfsfj.de/bmfsfj/service/publikationen/freiwilliges-engagement-in-deutschland-176834

[2] https://www.digitale-nachbarschaft.de/ueber-uns/ueber-das-projekt

[3] https://www.deutsche-stiftung-engagement-und-ehrenamt.de/dseeerklaert/

DSGVO-Compliance aus Sicht eines Vereins

Damit die Befassung mit Datenschutz in einem Verein zum Thema wird, muss als erstes ein Bewusstsein hierfür entstehen. Häufig sind es einzelne Aktive, die den Einsatz bestimmter digitaler Hilfsmittel hinterfragen: „Dürfen wir die Mitgliederliste einfach in die Dropbox packen?“, „Was muss man bei der Nutzung von Office 365 beachten?“, „Wie ist das jetzt eigentlich mit Zoom? Ist das DSGVO-konform oder nicht?“. Aber auch beim konkreten Handeln des Vereins entstehen Fragen: „Müssen wir uns etwas unterschreiben lassen, wenn wir auf einer Veranstaltung fotografieren?“, „Dürfen wir mögliche Interessenten für Veranstaltungen einfach so anschreiben?“, Wie lange dürfen wir Mitgliederdaten aufbewahren?“.

Um von der Befassung mit derartigen Fragestellungen zu echter Datenschutz-Compliance zu kommen, müssen zwei wichtige Perspektivwechsel stattfinden:

Zum einen muss der Blick von der einzelnen Verarbeitungstätigkeit hin zu einem Gesamtüberblick gerichtet werden. Zum anderen muss der Vereinsvorstand erkennen, dass Datenschutz ein zentrales Compliance-Thema ist und nicht durch einzelne Aktive singulär im Rahmen ihrer Aktivität bearbeitet werden kann. Dies zu erkennen kann abschreckend wirken und zu einer „den Kopf in den Sand stecken“-Mentalität führen. Dieser Aspekt hat jedoch gar nicht so sehr mit den materiellen Anforderungen der DSGVO zu tun, sondern liegt vielmehr im Verantwortlichkeitsbegriff und der Rolle des Vorstands begründet.

Doch auch wenn dieser Perspektivwechsel vollzogen wurde und ausreichend Informationsquellen vorhanden sind, gibt es weitere Hürden: Zeit ist im ehrenamtlichen Engagement ein knappes Gut. Wer schon seine wertvolle Freizeit opfert, will den Einsatz für die Sache eher ungern mit Compliance-Themen ausbremsen. Dieser Aspekt taucht natürlich auch im unternehmerischen Kontext, in Form eines unerwünschten Kostenfaktors, auf. Dennoch hat Compliance im unternehmerischen Kontext eine andere Bedeutung als im ehrenamtlichen Engagement, wo individueller Einsatz stärker im Vordergrund steht.

Die Komplexität des Datenschutzrechts ist ein weiteres bremsendes Element. Um die weiter oben beispielhaft erwähnten Fragen zur Zulässigkeit einzelner Verarbeitungstätigkeiten zu beantworten, muss man recht tief in die Materie einsteigen und stößt dabei unweigerlich auf auslegungsbedürftige Begriffe und ungeklärte Rechtsfragen. Daher müssen die Antworten auf solche, aus Sicht der Fragestellenden vermeintlich einfachen Fragen, sehr komplex ausfallen. Auch dieser Aspekt ist nicht vereinsspezifisch, aber kommt hier stärker zum Tragen, da eine individuelle, fachliche Begleitung in den allermeisten Vereinen nicht vorhanden ist und auch nicht finanzierbar wäre.

Vereinsspezifische Fragestellungen bei der Auslegung von Normen

Bei der Auslegung von Normen tauchen teilweise auch Fragestellungen auf, welche sich im wirtschaftlichen Kontext in der Form gar nicht stellen. Ein schönes Beispiel hierfür ist die Personengrenze des § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG), wonach ein Datenschutzbeauftragter zwingend zu benennen ist, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Über Sinn und Zweck dieser Regelegung in Form eines konkreten Schwellwerts wird viel diskutiert. Häufig wird argumentiert, dass diese Norm des bundesdeutschen Gesetzgebers, im Gegensatz zu den risikobasierten Regelungen der DSGVO, eine höhere Klarheit in der Rechtsanwendung schaffe.

Bei Vereinen erhöht diese Norm die Unsicherheit jedoch enorm. Zum einen ist der hier weit auszulegende Beschäftigtenbegriff, anders als im unternehmerischen Kontext, im Kontext von Vereinen alles an-

[4] https://stiftungdatenschutz.org/ehrenamt

29

PRIVACYSOFT
Datenschutzmanagement as a Service

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

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

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

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

BvD e.V. MITGLIED
DATENSCHUTZ GESTALTEN

EXKLUSIV FÜR BvD-MITGLIEDER
DATENSCHUTZ-AWARENESS-ONEPAGER
Fordern Sie einfach und kostenlos unter www.privacysoft.de an.
Code: ONEPAGERBVD2022

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

dere als intuitiv. Dass hier sämtliche für den Verein tätige Personen, unabhängig von Vereinsmitgliedschaft, Anstellungsverhältnis oder Bezahlung, hinzuzuzählen sind, überrascht Vereinsverantwortliche. Dieses potentielle Missverständnis ist durch entsprechende Erläuterungen noch vergleichsweise einfach aufzuklären.

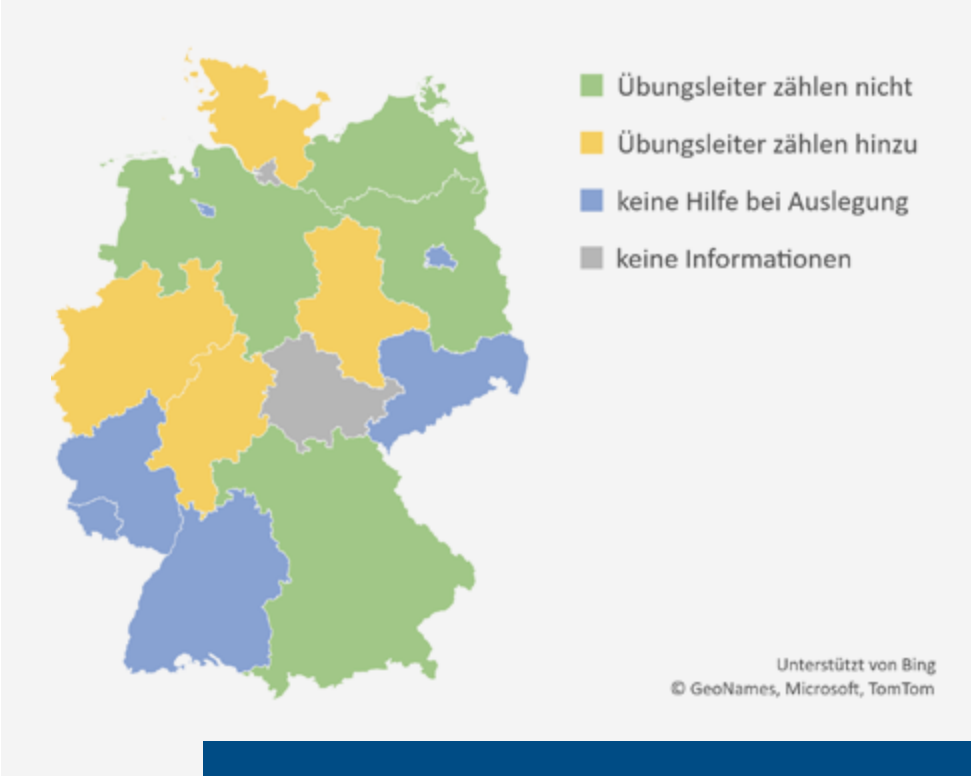
Höchst unglücklich wird es bei der Frage, welche Form der Tätigkeit für den Verein erforderlich ist, um die Kriterien „in der Regel" und „ständig" zu erfüllen. Im Gegensatz zu Unternehmen, bei denen Vollzeitbeschäftigung noch immer die Regel ist, finden Tätigkeiten für einen Verein fast immer in Teilzeit statt. Im Kontext ehrenamtlichen Engagements zumeist sogar nur kleinste Bruchteile einer regulären wöchentlichen Arbeitszeit. Der Unterschied zwischen einer Kopfzählung und einer Zählung in Form von Vollzeitäquivalenten ist im Fall der meisten Vereine daher enorm. Dass hier dennoch von einer Kopfzählung auszugehen ist, ist herrschende Meinung in der Literatur und wird auch von den Aufsichtsbehörden so vertreten.

Der zweite Aspekt dieser Fragestellung betrifft die Frage der Tätigkeiten der in Frage stehenden Personen. Von Mitarbeitenden einer Geschäftsstelle abgesehen, spielt die automatisierte Datenverarbeitung bei den allermeisten Vereinen nur eine untergeordnete Rolle. Ob eine solche Tätigkeit, welche nicht zur Kernaufgabe der Person gehört und in vielen Fällen auch nur gelegentlich erfolgt, dennoch das Kriterium der ständigen Beschäftigung erfüllt, ist umstritten.

Auch die Aufsichtsbehörden scheinen in dieser Frage uneins zu sein. Das DSK-Kurzpapier Nr. 12[5] gibt in Bezug auf die Regelungen des § 38 Abs. 1 BDSG nur den Gesetzeswortlaut wieder und hilft daher nicht weiter. Mit Ausnahme von Thüringen und Hamburg sind jedoch bei allen Aufsichtsbehörden der Länder Informationen zur nationalen Benennungspflicht zu finden. In Berlin und Brandenburg nur in allgemeiner Form zur Benennungspflicht von DSB, bei allen anderen sogar als Teil der vereinsspezifischen Informationsmaterialien.

Teils sind die Ausführungen mit Positiv- und Negativbeispielen aus dem Vereinskontext versehen. Übungsleiter oder Sporttrainer, dessen Hauptaufgabe im Training und nicht in der Verarbeitung der Mannschaftsliste liegen, werden von einigen Aufsichtsbehörden explizit als Negativbeispiel genannt. Vereine, die Informationsmaterialien dieser Bundesländer lesen, kommen somit zum Schluss, dass diese für die 20-Personen-Grenze nicht mitgezählt werden müssen. Andere Aufsichtsbehörden nennen diese Personen wiederrum als Beispiele für Personen, die hinzugezählt werden müssen oder weisen lediglich darauf hin, dass Umfang und Intensität der Datenverarbeitung irrelevant sind. In diesen Fällen dürften Vereine also zu dem Schluss kommen, dass diese für die 20-Personen-Grenze mitgezählt werden müssen. Ein Teil der Aufsichtsbehörden gibt auch nur den Wortlaut des § 38 BDSG wieder oder weist auf die ungeklärten Fragen hin, so dass deren Materialien Vereinen in dieser Frage nicht weiterhelfen.

Dieses sehr gemischte Bild ist nachstehend visualisiert.



Informationen der Aufsichtsbehörden zur Frage von Übungsleitern als ständig mit Datenverarbeitung beschäftigten Personen.

Problematische Folgen durch Unsicherheit

Die äußerst diffuse Informationslage zur Benennungspflicht von Datenschutzbeauftragten im Kontext von Vereinen ist deshalb problematisch, da Vereine in ihren Bemühungen zur Datenschutz-Compliance unnötig behindert werden. Dass es eine Benennungspflicht gibt, ist recht weit bekannt, so dass sich viele Vereinsaktive die Frage stellen, ob ihr Verein unter diese Pflicht fällt. Stoßen sie nun auf auslegungsbedürftige

[5] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_12.pdf

oder gar widersprüchliche Informationen, kann Resignation einsetzen, die nicht nur diese Frage, sondern die gesamte DSGVO-Umsetzung betrifft.

Diesem Aspekt wird in der regelmäßig wiederkehrenden Diskussion um die nationale Benennungspflicht kaum Aufmerksamkeit geschenkt. Die zentrale Fragestellung ist meistens, ob eine Erhöhung bzw. Absenkung dieser Personengrenze zu einer tatsächlichen Entlastung im Datenschutz führen kann oder nur zu einem Wegschauen durch Verantwortliche führt, da sie nicht durch fachkundige Personen in der Umsetzung begleitet werden. Die debattierten Lösungsmöglichkeiten umfassen daher meist keine Konkretisierungen der Norm, sondern drehen sich um die Anzahl der Personen, eine komplette Streichung der Regelung oder die Einführung anderer Kriterien.

Die hohe Auslegungsbedürftigkeit der Norm könnte durch den Bundesgesetzgeber jedoch ohne weiteres adressiert werden, indem Legaldefinitionen für die verwendeten Begriffe in das BDSG aufgenommen werden. Das BDSG a.F. enthielt in § 3 immerhin noch eine Definition für den Begriff der automatisierten Verarbeitung, die in der seit dem 25. Mai 2018 gültigen Fassung nicht mehr enthalten ist. Doch obwohl die Unbestimmtheit der verwendeten Begriffe in der Kommentarliteratur diskutiert wird, wird dies scheinbar nicht als Problem der Norm aufgefasst. Die im Oktober 2021 veröffentlichte Evaluation des BDSG durch die Bundesregierung enthält keinerlei Auseinandersetzung zu dieser Frage. Lediglich die Sinnhaftigkeit der kopfzahlbasierten Berechnung der Personenzahl wird dort diskutiert.[6]

Der kürzlich vom Freistaat Bayern in den Bundesrat eingebrachte Antrag[7] schlägt eine erneute Anpassung der nationalen Benennungspflicht vor. Interessanterweise steht dort aber nicht eine Anhebung der Personenzahl zur Debatte, sondern es wird eine Beschränkung auf Personen, deren Kerntätigkeit in Verarbeitungen gemäß Art. 37 Abs. 1 lit. b) und c) DSGVO liegt, vorgeschlagen. Hiermit solle der risikobasierte Ansatz der DSGVO in der nationalen Regelung zur Benennungspflicht umgesetzt werden. Für Vereine würde eine entsprechende Änderung tatsächlich eine klarere Auslegung der Benennungspflicht bedeuten, da nur sehr wenige Vereine Personen mit entsprechenden Kerntätigkeiten beschäftigen dürften.

Gleichzeitig enthält der bayerische Antrag einen Vorschlag, der Ausnahmen für ehrenamtlich Engagierte von der nationalen Benennungspflicht schaffen soll. Dort ist von nichtgewerblich tätigen Vereinen, gemeinnützigen Unternehmen und gemeinnützigen Dienstleistungen als Abgrenzungsmerkmalen die Rede. Je nach konkreter Ausgestaltung würde dies erneut massives Potenzial für Unklarheiten bei der Auslegung der Norm mit sich bringen. Im schlimmsten Fall müsste dann noch zusätzlich zwischen den Tätigkeiten von Personen in den sogenannten vier Sphären gemeinnütziger Organisationen unterschieden werden. Eine solche Regelung könnte die Unsicherheit im Umgang mit der Norm somit erhöhen, obwohl sie eine Erleichterung für ehrenamtlich Engagierte schaffen soll.

Weitere Beispiele für Unklarheiten im Kontext von Vereinen

Die nun recht ausführlich durchgeführte Betrachtung steht exemplarisch für eine Vielzahl von Fragestellungen, bei denen sich in Vereinen und in anderer Form Engagierte mit der Komplexität des Datenschutzrechts konfrontiert sehen. Fachliche Begleitung in Form eines Datenschutzbeauftragten haben nur die wenigsten Vereine und in den meisten Fällen sind es pflichtbewusste Vorstände oder Aktive, die sich selbst an der Auslegung der Normen versuchen. Diese Problematik kommt zur hohen Anzahl an Pflichten, welche die DSGVO bereithält und den Anforderungen der praktischen Umsetzung, wie im Fall der Informationspflichten, hinzu.

Die Unklarheiten rund um das Zusammenspiel von DSGVO und Kunsturhebergesetz (KunstUrhG) beim Veröffentlichen von Fotos sind ein weiteres Beispiel, welches im Vereinskontext höchst relevant ist. Die Dokumentation in Form von Fotos spielt in vielen Vereinen eine bedeutende Rolle und die Unsicherheiten in diesem Bereich führen bereits zu Abschreckungseffekten (sogenannte chilling effects), bei denen Vereine ihre Aktivitäten aus Unsicherheit vor gesetzlichen Vorgaben einschränken. So erreichen uns nicht nur Fragen, ob und unter welchen Voraussetzungen Fotos angefertigt werden dürfen, sondern auch ob die fotografische Dokumentation der letzten Jahrzehnte nun vernichtet werden müsse.

Ein weiteres Beispiel einer nationalen Regelung, deren Auslegung im Fall von Vereinen eine größere Komplexität mit sich bringt, ist die Frage der Anwendbarkeit des Gesetzes gegen den unlauteren Wettbewerb (UWG). Vereine wollen verständlicherweise für ihre Sache werben und bedienen sich hierzu häufig auch Formen der direkten Ansprache, welche eine unzumutbare Belästigung gemäß § 7 UWG darstellen kann. Bei Vereinen stellt sich allerdings die Frage, ob diese überhaupt in den Anwendungsbereich des UWG fallen, da die Vereinsaktivität in vielen Fällen keine geschäftliche Handlung im direkten Sinne darstellt, aber mittelbar zu einer Absatzförderung weiterer Marktteilnehmer führen kann. Ein viel grundsätzlicherer Bereich ist die Prüfung des berechtigten Interesse gemäß Art. 6 Abs. 1 lit. f) DSGVO. Der Spielraum für Datenverarbeitung auf Basis der Vereinssatzung als Vertrag mit den

[6] https://www.bmi.bund.de/SharedDocs/evaluierung-von-gesetzen/downloads/berichte/evaluierung-bdsg.pdf?__blob=publicationFile&v=3, Kapitel 5.5.3.2

[7] https://dserver.bundestag.de/brd/2022/0202-22.pdf

STIFTUNG DATENSCHUTZ

Seit Mai 2021 widmet sich die Stiftung Datenschutz in einem neuen Schwerpunkt Vereinen und ehrenamtlich Engagierten. Unter der Bezeichnung „Datenschutz im Ehrenamt“ bietet sie monatliche Webinare, schriftliche Informationen zur praktischen Datenschutzumsetzung und einen Generator für Datenschutzhinweise. Im Basiswissen werden die DSGVO-Grundlagen erläutert und Grundbegriffe geklärt. Der Praxisratgeber vertieft dieses Wissen und hilft bei der praktischen Umsetzung anhand kon-kreter Beispiele aus dem Vereinsalltag. In einem Newsletter wird die Zielgruppe über die Aktivitäten aus dem Bereich informiert.

- https://stiftungdatenschutz.org/ehrenamt
- https://social.bund.de/@DS_Stiftung
- https://twitter.com/DS_Stiftung/

Die Stiftung Datenschutz wurde 2013 von der Bundesregierung gegründet. Sie agiert als unabhängige Informations- und Diskussionsplattform. Mit Veranstaltungen wie dem DatenTag und dem DatenDialog bietet sie eine Diskussionsplattform zu Fragen der Datenpolitik. Daneben informiert sie zur Umsetzung des Datenschutzrechts in der Praxis. Die Bundestiftung versteht sich als Schnittstelle zwischen Politik, Aufsichtsbehörden, Wirtschaft, Wissenschaft und Gesellschaft. Die Stiftung ist gemeinnützig und neutral. Ihre Arbeit wird aus dem Bundeshaushalt gefördert.

Mitgliedern ist meistens sehr begrenzt. Vieles von dem, was das Vereinsleben ausmacht und gängige Praxis ist, beinhaltet Datenverarbeitungen, die im Rahmen eines berechtigten Interesses liegen können. Die hierfür notwendige Interessenabwägung durchzuführen, ist jedoch dermaßen komplex, dass viele Vereine hiervor zurückschrecken und im Zweifel lieber auf Einwilligungen setzen. Aufsichtsbehörden und Anwälte, welche die hohen Anforderungen der Prüfung betonen, tragen dazu bei, dass oftmals unnötige und den formellen Anforderungen nicht genügende Einwilligungen eingeholt werden. Ob dies die Rechtssicherheit der Vereine wirklich erhöht, ist diskussionswürdig. In jedem Fall trägt es zur allseits bekannten Einwilligungsmüdigkeit bei und erzeugt ein nicht gerade konstruktives Bild vom Datenschutz.

Schlussfolgerungen und Handlungsoptionen relevanter Akteure

Die hier aufgeführten Beispiele verdeutlichen, dass im Kontext ehrenamtlichen Engagements nicht nur die materiellen Anforderungen der DSGVO eine hohe Hürde mit sich bringen, sondern auch bei der Auslegung von Normen Schwierigkeiten entstehen. Dies hängt zum einen mit spezifischen Konstellationen ehrenamtlich betriebener Organisationen zusammen, welche bei der Gesetzgenese nur eine untergeordnete Rolle spielen. Aber auch in Fällen, in denen Vereine bei der Anwendung der DSGVO vor denselben Herausforderungen wie Unternehmen stehen, existiert ein wichtiger Unterschied: Es sind nur in seltenen Fällen Möglichkeiten für qualifizierte Einzelfallberatung vorhanden.

Unabhängig von der Frage, ob aufgrund formeller Anforderungen ein Datenschutzbeauftragter benannt werden müsste – die meisten Vereine haben keinen. Selbst wenn sie sich der Erforderlichkeit dessen bewusst wären, müssten die finanziellen Mittel hierfür aufgebracht werden und entsprechende Kapazitäten am Markt vorhanden sein. Bei punktueller Beratung zu einzelnen Fragen ohne die dauerhafte Benennung eines Datenschutzbeauftragten sieht es nicht anders aus. Folglich müssen die meisten Vereine auf interne Ressourcen zurückgreifen, was wiederrum gute Informationsmöglichkeiten und ausreichende zeitliche Kapazitäten voraussetzt.

Die Datenschutzaufsichtsbehörden der Länder tragen mit ihren Informationsangeboten bereits einen Teil zu den Informationsmöglichkeiten für Vereine bei. Inhaltliche Diskrepanzen, wie beim oben diskutierten Beispiel der nationalen Benennungspflicht, stiften dabei aber zusätzliche Verwirrung. Vereinen ist es nicht vermittelbar, dass zwei Sportvereine ähnlicher Größe aufgrund von Mannschaftslisten in einem Bundesland der Benennungspflicht unterliegen sollen und im anderen nicht. Hier ist eine bessere Abstimmung notwendig.

Politisch könnte für Vereine auch einiges erreicht werden, indem der Gesetzgeber für Klarstellungen in relevanten Bereichen sorgt. Oft werden auf Bundesebene Bereichsausnahmen für ehrenamtliches Engagement gefordert, was aufgrund des europarechtlichen Kontexts und den Vorgaben der Grundrechtecharta keine Option ist. Anstatt sich in der Diskussion auf Bereichsausnahmen oder Erleichterungen anderer Art zu versteifen, könnte mit einem Fokus auf die leichtere Anwendbarkeit durch klarere Auslegung bereits einiges erreicht werden.

Verbände, welche auch als politische Interessenvertretung von Vereinen fungieren, beteiligen sich gerne an den Forderungen nach Bereichsausnahmen für ehrenamtliches Engagement. Doch gerade ihnen kommt eine bedeutende Rolle im Aufzeigen von gangbaren Lösungen für ihre Mitgliedsorganisationen zu. Mit guten Mustern und Informationspaketen haben sie die Möglichkeit kniffelige Fragen des Datenschutzrechts für eine ganze

Gruppe an Vereinen zu beantworten, die sich ansonsten alle Vereine einzeln stellen müssen. Verhaltensregeln gemäß Art. 40 DSGVO wären darüber hinaus eine Möglichkeit die etablierte Praxis im Handeln der einzelnen Vereine, aber auch im Zusammenspiel mehrerer Vereine innerhalb der Verbandsstruktur, auf solide Füße zu stellen.

Insgesamt scheinen die Unterstützungsmöglichkeiten für Vereine und ehrenamtlich Engagierte stark ausbaufähig. Dass sich hier, im Gegensatz zur Wirtschaft und dem öffentlichen Bereich, weniger Strukturen herausgebildet haben, erstaunt angesichts der schwachen Finanzmittel im Bereich des freiwilligen Engagements nicht allzu sehr. Bedenkt man jedoch, dass mehr als ein Drittel der Bevölkerung Deutschlands freiwillig engagiert ist und sich direkt oder indirekt mit der DSGVO-Anwendung im jeweiligen Bereich befassen müsste, wird die Notwendigkeit hierfür deutlich. Denn rein zahlenmäßig sind die etwa 45 Millionen Erwerbstätigen[8] in Deutschland keine so viel größere Gruppe, als die der freiwillig Engagierten.

Über den Autor

Hendrik vom Lehn
ist Diplom-Informatiker mit einem Master-Abschluss in Technischer Politikfeldanalyse sowie Zertifizierter Berater im Datenschutzrecht (FernUniversität in Hagen). Er schult Vereine seit mehreren Jahren in der DSGVO-Umsetzung und ist als Datenschutzbeauftragter eines Vereins selbst ehrenamtlich engagiert. Bei der Stiftung Datenschutz gestaltet er Webinare für Vereine und hat den Bereich Datenschutz im Ehrenamt aufgebaut.

STIFTUNG DATENSCHUTZ

[8] https://www.destatis.de/DE/Themen/Arbeit/Arbeitsmarkt/Erwerbstaetigkeit/_inhalt.html

Anzeige

DATENSCHUTZ | DIGITAL PRODUCT SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

Online-eLearning zum Datenschutz

Die einfache Art, Ihre Beschäftigten zu sensibilisieren und nachweislich zu schulen!

> 11 Sprachen – Deutsch, Englisch, Chinesisch, Spanisch, Französisch, Portugisisch, Polnisch, Ungarisch, Italienisch, Tschechisch, Rumänisch, weitere Sprachen auf Anfrage
> Sofort einsatzbereit – kurzfristiger weltweiter Zugriff über Webbrowser, kein Verwaltungsaufwand
> Kostengünstig – flexibles Preismodell nach Unternehmensgröße. Einzelne, zeitlich befristete Schulungs-Kampagnen möglich
> Aktualisierungsservice – Updates für alle Sprachen unter Berücksichtigung aktueller Themen inkl. Austausch von Prüfungsfragen
> Schulungsnachweise – zentrale Rückmeldung über bestandene Teilnahme und Zertifikat zum Download für die Beschäftigten
> Erweiterungsmodul – Inhalte zur Informationssicherheit ebenfalls in deutsch und englisch verfügbar!
> Lernmanagement-System vorhanden? Alternativ sind alle Inhalte und Sprachen als Scorm-Dateien zum Import in Ihr System verfügbar

ditis TRAINING CENTER
SKILLED FOR THE DIGITAL FUTURE

Weitere Informationen, alle Inhalte und Sprachen zum Testen unter
https://eLearning.ditis.de
Jens Maschke, Tel. +49 7321 37 7384, jens.maschke@ditis.de

ditis Systeme – Niederlassung der JMV GmbH & Co. KG • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 15 • 89081 Ulm • www.ditis.de

DATENHERAUSGABE UND INFORMATIONS-FREIHEIT BY DESIGN

Was (nicht nur behördliche) Datenschutzbeauftragte wissen sollten.

Dr. Marit Hansen, Henry Krasemann

1. Von Informationsfreiheit zur europäischen Datenstrategie

„Öffentliche Daten nützen, private Daten schützen“ – dieses Motto gehört seit den 1980er Jahren zur „Hackerethik“ des Chaos Computer Clubs.[1] Dass Daten der öffentlichen Verwaltung auf Anfrage herausgegeben oder proaktiv bereitgestellt werden sollen, sofern nicht definierte private oder öffentliche Interessen dem entgegenstehen, haben Politik und Gesetzgebung vielerorts erkannt. Auf Ebene des Bundes und der überwiegenden Zahl der Länder gibt es Informationsfreiheits- oder Transparenzgesetze, die dazu Regeln vorgeben. In diesen Gesetzen ist auch festgelegt, wer auf Bundes- oder Landesebene die Ombuds-Rolle einer oder eines Informationsfreiheitsbeauftragten ausfüllen soll: Ausnahmslos sind dies in Deutschland der Bundesbeauftragte beziehungsweise die jeweiligen Landesbeauftragten für Datenschutz. Hier manifestiert sich bereits die Nähe von Datenschutz und Informationsfreiheit, die – soweit personenbezogene Daten betroffen sind – in einem Spannungsverhältnis stehen, das es in der Praxis aufzulösen gilt.

Für die Datenschutzbeauftragten in Behörden gehört die Beschäftigung mit den Abläufen, die das Informationsfreiheitsrecht verlangt, zu den Pflichtaufgaben – jedenfalls wenn die betroffenen Daten nicht offensichtlich ohne Personenbezug sind. Aber auch auf die Datenschutzbeauftragten in Unternehmen kommen derartige Aufgaben zu, wie sich aus der europäischen Datenstrategie[2] ergibt:

„Die EU schafft einen Binnenmarkt für Daten, in dem

- Daten innerhalb der EU und branchenübergreifend zum Vorteil aller weitergegeben werden können,
- europäische Vorschriften, insbesondere zum Schutz der Privatsphäre und zum Datenschutz, sowie das Wettbewerbsrecht in vollem Umfang eingehalten werden,
- die Regeln für Datenzugang und Datennutzung gerecht, praktikabel und eindeutig sind.“

Die Reihe von europäischen Rechtsakten, die zur Umsetzung dieser Strategie dienen sollen und sich zurzeit im Gesetzgebungsverfahren befinden, umfasst beispielsweise den Data Act, den Data Governance Act, den Digital Markets Act, den Digital Services Act und die Regelungen zu sektorspezifischen Datenräumen. Das bedeutet im Ergebnis: Die herausgabepflichtigen Stellen sollen ausgeweitet und deren Daten zunehmend genutzt, geteilt und zusammengeführt werden, ohne dass die vorgeschriebenen Datenschutzgarantien gefährdet sind. Diese Kultur der Informationsnutzung wird nicht nur Daten betreffen, bei denen von vornherein klar ist, dass kein Personenbezug besteht. Stattdessen nimmt die Diskussion um geeignete Verfahren zur Anonymisierung oder Pseudonymisierung erneut Schwung auf.

Insgesamt liegt nahe, die Anforderungen von Artikel 25 der Datenschutz-Grundverordnung – Datenschutz durch Technik-

[1] https://www.ccc.de/de/hackerethics

[2] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

gestaltung und durch datenschutzfreundliche Voreinstellungen – anzulegen, also Datenschutz by Design auch für Prozesse der Datenherausgabe zu realisieren. Selbstverständlich muss dies mit den gesetzlichen Informationsfreiheitspflichten kompatibel sein, d. h. eine falsch verstandene Datenminimierung („lieber gar nichts herausgeben") würde das Recht auf Informationszugang unterlaufen. Beiden Pflichten – Datenschutz auf der einen Seite und Informationsfreiheit bzw. Datenweitergabe im Sinne der europäischen Datenstrategie auf der anderen Seite – liegen Daten und Verarbeitungsprozesse zugrunde. Hier gilt es, einerseits im Vorfeld und andererseits immer wieder während der Verarbeitung („sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung" – Art. 25 Abs. 1 DSGVO) deren Gestaltung in den Blick zu nehmen. Es geht um „Datenschutz by Design & Informationsfreiheit by Design", wobei auch das Auflösen von etwaigen Spannungen zwischen den Anforderungen mitzubedenken ist.[3]

Ausgehend von den heutigen Informationsfreiheitsgesetzen wird im nächsten Abschnitt erklärt, welche organisatorischen Prozesse und technischen Unterstützungen für die typischen Fragestellungen einer Datenherausgabe sinnvoll sind und wo jeweils Datenschutzaspekte tangiert werden. Anschließend wird zusammengefasst, was diese – teilweise neuen – Anforderungen für die Arbeit der Datenschutzbeauftragten bedeuten.

2. Informationsfreiheit by Design

Informationsfreiheit für öffentliche Stellen propagiert die Freigebigkeit einer Datenherausgabe – unter Wahrung der öffentlichen und privaten Interessen: Die meisten Bundesländer und auch der Bund gewähren allen Menschen (und ggf. juristischen Personen) das Recht, die Herausgabe von Informationen bei öffentlichen Stellen zu verlangen, ohne dass hierfür ein gesondertes Interesse nachgewiesen werden muss. In ihrer Zielrichtung sind sich die Informationsfreiheitsgesetze einig: mehr Transparenz über das Behördenhandeln und damit Nachvollziehbarkeit von Entscheidungen. Inzwischen werden die Gesetze zu modernen Transparenzgesetzen umgestaltet, die die Stellen verpflichten proaktiv Informationen in Transparenzportalen zu veröffentlichen. Hierzu gehören auch die offenen Daten („Open Data"), also staatlich gesammelte Messwerte und Erhebungen, die frei etwa für Forschungsvorhaben genutzt werden können.

Für viele Behörden war (und ist immer noch) die Pflicht zur Informationsfreiheit eine ungewohnte Form der Transparenz. Wird ein entsprechender Antrag gestellt, bedeutet das nicht selten Stress für alle Beteiligten: Zuständigkeiten müssen geklärt werden, Informationen werden zusammengetragen, und es muss beurteilt werden, welche Informationen in welcher Form herausgegeben werden müssen – und welche einer Ausschlussregel unterfallen und daher z. B. zu schwärzen sind. Oft bleibt das ungute Gefühl, zu viel oder zu wenig weitergegeben zu haben. Dabei kann sich eine Behörde schon weit vor dem Antrag das Leben leichter machen und dennoch die Transparenzansprüche der Bürgerinnen und Bürger vollumfänglich erfüllen – durch Informationsfreiheit by Design. Dies wird heutzutage vor allem auf organisatorische Maßnahmen hinauslaufen. Aber auch technische Lösungen können bei der rechtmäßigen Beantwortung von Anträgen helfen.

a) Unternehmenskultur und Sensibilisierung

Oft unterschätzt wird die Bedeutung der Unternehmenskultur und Sensibilisierung der Mitarbeitenden für das Thema Informationsfreiheit. So gilt es, frühzeitig ein Bewusstsein zu schaffen, dass grundsätzlich alle Informationen in einer Behörde Informationsfreiheitsansprüchen und ggf. Veröffentlichungspflichten in Transparenzportalen unterliegen können. Das kann auch für intern verschickte Rundmails gelten, für Notizen und für Informationen auf Kommunikationsgeräten wie Tablet oder Smartphone. Wer beruflich handelt, erzeugt in der Regel amtliche Informationen. Zwar können in einzelnen Fällen Ausnahmen etwa für personenbezogene Informationen oder Mitteilungen mit rein internem Charakter gelten. Aber auch diese Ausnahmen greifen nur in eng umgrenzten Fällen. Die Regel ist, dass bei einer Behörde vorliegende Informationen herauszugeben sind.[4]

b) Strukturierte Informationshaltung

Die bequeme Datenherausgabe auf Knopfdruck ist zwar weitgehend Wunschdenken, doch kann man sich schon vorab so aufstellen, dass der Rechercheaufwand auf ein Mindestmaß beschränkt wird. Dazu gehört auch sich zunächst überhaupt klar darüber zu werden, wo Informationen vorhanden sind. Das sind in der Regel nicht nur die Datenbanken und Akten der Behörde, sondern auch externe Geräte wie Laptops, Tablets und Smartphones. Zudem schlummern viele Daten in E-Mail-Archiven. Auch aus Gründen des Datenschutzes ist es notwendig diese Informationsquellen abzugleichen, Erforderliches strukturiert zu speichern und Überflüssiges zu löschen. Dazu kann eine Unterscheidung zwischen völlig unproblematisch herausgebbaren Informationen und solchen mit Personenbezug/Betriebs- und Geschäftsgeheimnissen/Urheberschutz oder Ähnlichem vorgenommen werden.

Wer seine Daten so organisiert, ist nicht nur gut für Anträge nach dem Informationsfreiheitsrecht, sondern auch für Auskunftsansprüche nach Art. 15 DSGVO gerüstet.

[3] Marit Hansen, Felix Bieker, Benjamin Bremert: Datenschutz und Privatheitsschutz durch Gestaltung der Systeme, in: Michael Friedewald, Alexander Roßnagel (Hrsg.): Die Zukunft von Privatheit und Selbstbestimmung, DuD-Fachbeiträge, Springer, 2022, 259-300.

[4] Die Informationsfreiheitsrechte weisen diesbezüglich Unterschiede auf; es ist jeweils das einschlägige Informationsfreiheitsrecht anzulegen.

c) Festgelegte Zuständigkeiten und klare Abläufe

Anträge nach Informationsfreiheitsgesetzen sind keine überraschenden Schicksalsschläge, sondern es handelt sich um das Recht einer jeden natürlichen oder juristischen Person.

Wichtig sind klare Verfahrensabläufe mit entsprechenden Zuständigkeiten. Dies könnte wie folgt aussehen:

a) Sichtung des Antrags.
b) Prüfung: Richtiger Adressat des Antrags? Oder liegen die Informationen bei einer anderen Behörde, an die der Antrag weitergeleitet werden muss?
c) Prüfung: Antrag unklar? Dann Nachfrage bei der antragstellenden Person (ggf. mit Gebührenabschätzung).
d) Prüfung und Weiterleitung: Wer ist in der Behörde einzubinden?
e) Notieren und interne Kommunikation der Frist (i. d. R. ein Monat).
f) Recherche und Zusammenstellung der Informationen.
g) Prüfung von Ausschlussgründen inkl. ggf. Abwägung, Dokumentation.
h) Ggf. Anhörung von Betroffenen.
i) Ggf. Aufbereitung der Informationen (z.B. Schwärzung).
j) Ggf. Fristverlängerung mit Begründung.
k) Versand der Antwort (oder Termin zur Einsichtnahme).
l) Ggf. Einmeldung im Transparenzportal.
m) Ggf. Bearbeitung von Rückfragen.

So sollte klar geregelt sein, wer diese Anträge bearbeitet und federführend dafür sorgt, dass Antwortfristen (in der Regel ein Monat) eingehalten werden. Dies kann die bzw. der „Informationsfreiheitsbeauftragte“[5] der Behörde sein, wenn diese Funktion installiert wurde. Wichtig ist, dass auch ein(e) Vertreter(in) benannt wird, um bei längeren Ausfällen oder Urlaubszeiten die Fristen dennoch einhalten zu können. Je nach Größe der Behörde und der Verteilung der Zuständigkeiten sind die Fachabteilungen für die Beantwortung der Anfrage zu beteiligen. Zeit und Aufwand kann mit der Einbindung von Betroffenen einhergehen, wenn diese vor einer Datenherausgabe angehört oder um Zustimmung gebeten werden müssen.

d) Aufbereitung der Daten für die Herausgabe

Waren die bisher genannten Punkte eher auf organisatorische Maßnahmen für Informationsfreiheit by Design ausgelegt, so kann spätestens bei der Aufbereitung der Daten für die Herausgabe der Einsatz von Technik helfen. Unter anderem in der Verwaltung in Schleswig-Holstein ist ein System im Einsatz, das mit künstlicher Intelligenz (KI) personenbezogene Daten in einem Dokument erkennen und entsprechend zur Schwärzung markieren soll.

Das System lernt während des Betriebs dazu und verbessert seine Erkennungsrate. Derartige Systeme können eine große Hilfe bei der Bearbeitung von Anträgen darstellen, werden aber auf absehbare Zeit kein verlässlicher Automatismus werden: Dazu ist die Frage der Anonymität bzw. eines den Daten innewohnenden Personenbezugs zu komplex und geht weit über die Erkennung von Namen, Titeln und Adressen hinaus. Selbst wenn diese Informationen herausgelöscht werden, bedarf es aktuell noch menschlicher Intelligenz und Kreativität, um zu erkennen, ob z. B. aus der Gesamtschau des Textes ein Personenbezug ableitbar ist (etwa bei Ortsbeschreibungen) oder mittelbare Personenbeschreibungen (wie Beschreibung eines Nachbarschaftsverhältnisses) enthalten sind.

Hinzu kommt, dass nicht alle personenbezogenen und personenbeziehbaren Informationen vor der Weitergabe prinzipiell herauszunehmen sind. In der Regel verlangen die Informationsfreiheitsgesetze hierfür eine zusätzliche Abwägung zwischen den Interessen der betroffenen Personen und dem öffentlichen Bekanntgabeinteresse. Außerdem kann der Fall vorliegen, dass die informationspflichtige Stelle die Zustimmung der betroffenen Person vorab abfragen muss und dies in die Entscheidung über den Umfang der Herausgabe einfließen lassen muss.

[5] Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder regt die Einrichtung von Informationsfreiheitsbeauftragten an (https://uldsh.de/ifk-if-beauftragte). Im Koalitionsvertrag für die 20. Wahlperiode des Schleswig-Holsteinischen Landtages (2022-2027) der Regierungsparteien ist vorgesehen, in den Ressorts die Funktion von „Datenbereitstellungsnutzungsbeauftragten“ einzuführen.

Die (KI-)Systeme sollen künftig neben den personenbezogenen Daten auch bei anderen Ausnahmetatbeständen – etwa bei Betriebs- und Geschäftsgeheimnissen, internen Mitteilungen oder sicherheitsrelevanten Informationen – unterstützen. Auch wenn solche Systeme nicht alle Arbeit abnehmen können, so sind sie dennoch als Ergänzung hilfreich. Ihre Erkennung kann das Aufspüren vieler problematischer Textteile erleichtern, die Mitarbeitenden sensibilisieren und die Gefahr reduzieren, etwas übersehen zu haben – solange man sich dessen bewusst ist, dass auch noch menschliche Kontrolle erforderlich ist.

e) Art der Datenherausgabe

In der Regel obliegt es der antragstellenden Person zu wählen, welchen Weg der Datenherausgabe sie wünscht (etwa über E-Mail, Postversand, Einsichtnahme vor Ort). Je nach Art der Datenherausgabe sollte vorab verwaltungsintern geklärt und geregelt werden, was hierbei zu beachten ist. So werden bei Anträgen über die Webseite fragdenstaat.de Antworten der Behörde in der Regel zeitnah auf der Website veröffentlicht; auch auf privaten Websites werden solche Schreiben hochgeladen. Dies kann Auswirkungen darauf haben, welche Vorkehrungen eine informationspflichtige Stelle für den Schutz der Daten ihrer Mitarbeitenden vornimmt. So könnten Antworten über eine zentrale Stelle versendet werden und Informationen über die sachbearbeitenden Personen auf das Notwendige reduziert werden.

f) Bereitstellung im Transparenzportal

In einigen Bundesländern ist es für bestimmte Behörden verpflichtend, beantwortete Anfragen nach dem Informationsfreiheitsrecht in ein Transparenzportal einzustellen. Können aufgrund von Abwägungen oder Einwilligungen in der Antwort der Behörde noch personenbezogene und personenbeziehbare Informationen enthalten sein, so sind diese bei der Einmeldung in dem Transparenzportal in der Regel zu entfernen.

Dies gilt auch für Daten, die auf die antragstellende Person hinweisen. Auch hier können KI-Systeme unterstützen. Allerdings können schon Fragestil, Datum oder auch Informationsthema deutliche Hinweise auf die antragstellende Person geben, was KI-Systeme nicht vollständig erkennen können. Auch hier ist also menschliche Skepsis gefragt.

Zudem können Datenpannen nicht ausgeschlossen werden, und möglicherweise ergibt sich auch erst zu einem späteren Zeitpunkt, dass bereitgestellte Informationen einen Personenbezug aufweisen oder andere schutzwürdige Interessen verletzen. Für die dann notwendigen Reaktionen – zum Beispiel das Treffen risikomindernder Maßnahmen, gegebenfalls Melde- und Benachrichtigungspflichten – müssen die Mitarbeitenden sensibilisiert und geeignete Abläufe, verzahnt mit dem Datenschutzmanagement, definiert werden.

Veranstaltungshinweis

Die ULD veranstaltet seine diesjährigen Sommerakademie am 12. September in Kiel zum Thema „Informationsfreiheit by Design – und der Datenschutz?!“

Zu weiteren Informationen über das Programm und die Anmeldung gelangen Sie über den QR-Code.

3. Bedeutung für die Datenschutzbeauftragten

So wie „Datenschutz by Design“ frühzeitig im Entwicklungsprozess einer Datenverarbeitung ansetzen muss, gilt dies auch für das Einbauen anderer Anforderungen. Selbstverständlich sind solche Lösungen anzustreben, die sämtliche Anforderungen erfüllen. Was nicht von Anfang an im Pflichtenheft der Systementwicklung steht, muss ansonsten aufwendig oder kostenintensiv später nachgebessert werden – oder ist möglicherweise gar nicht realisierbar, sodass die Verfahren zur Verarbeitung als untauglich angesehen und völlig neu implementiert werden müssen. Problematisch wären auch spontane Workarounds, z. B. durch den Aufbau von Parallelsystemen neben der datenschutzgerechten Implementierung. Stattdessen sollte Wert auf ein planvolles Vorgehen gelegt werden, das auch der Kontrolle der oder des Datenschutzbeauftragten unterliegt.[6] Die Pflichten nach den Informationsfreiheitsgesetzen können für Datenschutzbeauftragte in den betroffenen Stellen zudem eine Chance darstellen: Sie bieten gute Argumentationsgrundlage dafür bisher kaum beachtete Datensammlungen wie in dienstlichen Smartphones, Tablets und Laptops in ein gesamtes Datenschutz- und Informationsfreiheitsmanagementsystem einzubinden und eine Gesamtrevision vorzunehmen. Organisatorische und technische „Informationsfreiheit by Design“ kann hierbei unterstützen, ohne dass dies zu einer überschnellen „Informationsfreiheit by Knopfdruck“ ohne jegliche Prüfung von rechtlich normierten Ausschlussgründen verkürzt wird. Menschliches Fachwissen und Risikobewusstsein müssen weiterhin eingebracht werden, doch der Aufwand für eine rechtskonforme Datenherausgabe kann maßgeblich reduziert werden.

Datenherausgabewünsche und -pflichten werden künftig so gut wie alle Bereiche betreffen. Es bietet sich an, dass Datenschutzbeauftragte die damit zusammenhängenden Punkte in ihrer Beratungs- und in ihrer Überwachungsfunktion (Art. 39 DSGVO) aufnehmen. Ziel ist es auch bei den verpflichtenden Datenherausgaben die Rechte und Freiheiten natürlicher Personen zu gewährleisten – und zwar am besten „by Design“.

Datenschutzbeauftragte sollten auf jeden Fall die folgenden Punkte im Blick haben:

- Ausreichende Kenntnis der für den Verantwortlichen geltenden rechtlichen Regelungen zu Datenherausgaben, soweit personenbezogene Daten tangiert sein können;
- Gestaltung der Verfahren zu solchen Datenherausgaben, dabei insbesondere Fragen zur Prüfung des Personenbezugs der Daten, zur Datenminimierung (etwa einer tauglichen Anonymisierung) und, wo dies eine Rolle spielt, zur Zweckbindung, sowie
- Sensibilisierung der daran beteiligten Mitarbeitenden für die Aspekte des Datenschutzes, insbesondere das Risiko für die Rechte und Freiheiten natürlicher Personen.

Über die Autoren

Dr. h.c. Marit Hansen
ist seit 2015 Landesbeauftragte für Datenschutz Schleswig-Holstein und damit Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Seit 1995 arbeitet die Informatikerin in der Behörde, im Jahr 2008 wurde sie stellvertretende Landesbeauftragte für Datenschutz. Marit Hansen war Mitglied in der Datenethikkommission der Bundesregierung. Im April 2020 erhielt sie für ihre Verdienste in datenschutzfreundlicher Systemgestaltung die Ehrendoktorwürde der Universität Karlstad, Schweden.

Henry Krasemann
ist seit 2002 juristischer Mitarbeiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein und leitet dort das Referat für Akkreditierung, Zertifizierung und Informationsfreiheit.

[6] Hier kann auch die Notwendigkeit einer Datenschutz-Folgenabschätzung bestehen, beispielsweise bei Anonymisierung von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, siehe auch https://uldsh.de/dsfa-muss-liste.

Anzeige

Empfohlen von

DATENSCHUTZ EXPERTE.DE

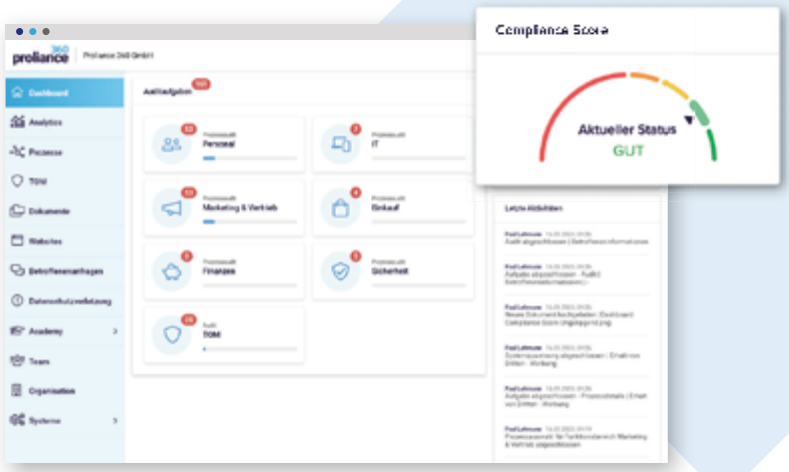
Ein Freimonat für BvD-Mitglieder

Automatisiertes Datenschutzmanagement mit Proliance 360

Datenschutz vorgedacht: Verabschieden Sie sich von Excel und Papier sowie manuellen Arbeitsschritten. Mit Proliance 360 haben Sie die DSGVO im Griff und Ihre Datenschutz-Compliance stets im Blick. Entwickelt mit der Erfahrung aus über 1.500 Kundenprojekten. Nie war es einfacher, Datenschutz zu managen.

Unser Angebot für Sie

- Das DSGVO-Komplettset: VVT, TOM, Schulungen & Co.
- Datenschutz auf Knopfdruck mit über 25.000 vorgedachten Workflows
- Aufwände für Datenschutzmanagement signifikant reduzieren
- Einfache Bedienung und Einbindung von Teammitgliedern



Weitere Informationen zu Proliance 360 finden sie auf **www.proliance.ai**
Vereinbaren Sie noch heute einen Beratungstermin unter **+49 (0)89 2500 392 20** oder buchen Sie Ihren Slot online mit Hilfe des **QR-Codes.**

PROLIANCE GmbH München, 2021

proliance

DIGITALFÜHRERSCHEIN MACHT FIT FÜRS NETZ

Dr. Michael Littger

Deutschland sicher im Netz e.V. vermittelt Wissen rund um die vernetzte Welt.

Folgt man dem Sicherheitsindex von Deutschland sicher im Netz e.V., benötigen aktuell über 60 Prozent aller Internetnutzenden praktische und verständlichere Hilfestellungen im Umgang mit der digitalen Welt. Denn Wissen und Kompetenzen im digitalen Alltag sind in einer sich immer weiter vernetzenden Welt mehr und mehr gefragt – doch längst nicht alle Bürger:innen können mit den fortlaufenden Entwicklungen Schritt halten. An diesem Punkt setzt der DsiN-Digitalführerschein (DiFü) an.

Sich sicher und kompetent im Netz bewegen – das bedeutet für jede:n etwas anderes. Viele Verbraucher:innen können zwar souverän mit Internet und Co. umgehen und wissen, wo potenzielle Risiken drohen. Die Hintergründe solcher Risiken kennen sie jedoch nur bedingt und wissen oft nicht, wie derartige Gefahren ihnen im Alltag begegnen. Kurz: Wir nutzen digitale Möglichkeiten zu unbedarft und bewegen uns zu fahrlässig im Internet. Dabei wird es immer wichtiger zu wissen, welche Gefahren konkret existieren, und was die sichersten Mittel sind, um sich dagegen zu schützen.

Doch nicht nur Risiken und Gefahren stehen im Fokus: Die digitale Welt bietet auch eine Vielzahl an Chancen und Möglichkeiten. Wer sich nicht auskennt, nimmt diese jedoch schlichtweg nicht wahr. Der DsiN-Digitalführerschein ist eine Reaktion auf das immer stärker werdende Aufklärungsbedürfnis und setzt an diesem Punkt an. Vor allem für die berufliche Zukunft ist es von immer größerer Bedeutung sich sicher in der digitalen Welt bewegen zu können. Denn diese wird fortlaufend komplexer, mit den neusten Entwicklungen mitzuhalten ist daher dringend notwendig. Das Bildungsangebot des DsiN-Digitalführerscheins vermittelt Grundlagen und weiterführendes Wissen. Verbraucher:innen können dieses testen, erweitern und zertifizieren lassen.

Individuelle Weiterbildung durch vielseitiges Lernangebot

Wie mit E-Mail-Anhängen von unbekannten Absendern umgehen? Was tun bei Belästigung im Netz? Welche Möglichkeiten zum sicheren Bezahlen bei Online-Einkäufen gibt es? Diese und weitere Fragen stellen sich Verbraucher:innen aller Altersstufen. Je nach Präferenz kann das Lernangebot im privaten oder beruflichen Kontext absolviert werden.

Da es von Bedeutung ist zuerst einmal den eigenen Wissens- und Kenntnisstand zu kennen, um sich entsprechend weiterbilden zu können, wird das individuelle Kompetenzniveau mithilfe einer Selbsteinschätzung ermittelt und entsprechend eines von drei Kompetenzniveaus ausgewählt: Entdecker:in, Erfahrene:r oder Alleskönner:in. Anschließend werden die sechs Themenbereiche Geräte, Internet, Kommunikation, Datenwelt, Gefahrenschutz und Technologiealltag durchlaufen. Diese behandeln Fragen und Herausforderungen in Bezug auf digitale Grundlagen, Datenschutz und Sicherheit bis hin zu digitalen Tools im Alltag. Der eigene Wissens- und Kompetenzerwerb kann dabei jederzeit unterbrochen werden, um direkt zur abschließenden Prüfung zu gelangen. Am Ende der Prüfung, die alternativ in mehreren Teilschritten absolviert werden kann, steht die Ausstellung eines Zertifikats, das die erbrachten Leistungen in den einzelnen Themenbereichen detailliert aufzeigt. Dieses verfügt über Verifizierungsmöglichkeiten via SMS oder QR-Code.

Mehr Datenschutzkompetenz durch vertiefende Themenbereiche

Wer seine Daten richtig schützen möchte, muss vor allem wissen, worauf dabei genau geachtet werden sollte. Neben dem Wissen darüber, was Datenschutz eigentlich bedeutet, sind folgende vier Kernbereiche essentiell, die im Lernangebot im Bereich „Datenwelt“ vertiefend erläutert werden: Datensparsamkeit, Logins & Passwörter, Backups sowie Clouds.

1. Datensparsamkeit meint den verantwortungsvollen Umgang mit persönlichen Daten im Internet – egal, ob es sich um die eigenen oder die von Familienmitgliedern, Freund:innen und Bekannten handelt. Denn je weniger Daten bei Onlineanbietern gespeichert sind, desto weniger Daten können Hacker:innen missbrauchen, stehlen und an Unbefugte weitergeben. Für Onlinedienste in der EU ist Datensparsamkeit aufgrund der DSGVO Pflicht. Anbieter dürfen also nur persönliche Daten abfragen und speichern, die für die Nutzung ihrer Dienste notwendig sind und müssen sie löschen, sobald sie sie nicht mehr benötigen.

2. Logins und Passwörter sind ähnlich wie ein Schlüssel zu einem Safe: Beim Einloggen identifiziert man sich als diejenige Person, die berechtigt ist, auf die persönlichen Daten eines bestimmten Kontos, Profils oder Accounts zuzugreifen. Denn dabei handelt es sich um vertrauliche Daten, die nicht für jede:n zugänglich sein dürfen. Passwortmanager unterstützen dabei ausreichend komplexe Passwörter für diverse Websites erstellen und zu speichern. Zusätzliche Login-Bestätigungen durch Zwei-Faktor-Authentisierung (2FA) oder U2F-Sticks sorgen für erweiterten Schutz.

3. Der USB-Stick zerbricht oder der Laptop ist nicht mehr funktionstauglich? Mithilfe von Backups lassen sich Dateien oder ganze Betriebssysteme entweder auf externe Datenträger oder in der Cloud speichern. Sicherheitskopien auf externen Datenträgern können jedoch nur dann umfänglich vor Datenverlust schützen, wenn diese stets mit den Originalen synchronisiert und somit aktuell gehalten werden. Die regelmäßige Datensicherung kann jedoch dauerhaft recht mühsam sein. Eine Lösung sind Tools zur Automatisierung des Synchronisierungsprozesses. Die Verschlüsselung von Dateien oder ganzer Laufwerke bietet dabei gewissen Schutz vor Hacker:innen, Diebstahl sowie Kinder- und Jugendschutz.

4. Clouds bieten vereinfacht gesagt die Funktion das Speichern zu erleichtern. Dies kann vor allem bei Backups nützlich sein. In Clouds können Dateien sowie gesamte Betriebssysteme hochgeladen werden - so kann man mit jedem neuen Computer auf sein altes Betriebssystem mit all seinen Programmen, Dateien oder Sicherheitsvorkehrungen wieder zugreifen.

Neben den Grundlagen rund um den Datenschutz selbst sollten sich Verbraucher:innen vor allem mit bestehenden Risiken und Gefahren befassen. Um sich optimal zu schützen, lohnt es sich tiefgreifender mit den folgenden Themen auseinanderzusetzen: Updates, Schadsoftware, Social Engineering, Doxxing, Identitätsdiebstahl und Scam.

1. Egal welche Software man nutzt: Jedes Programm und jedes Betriebssystem braucht Updates. Damit werden Fehler behoben, Sicherheitslecks geschlossen und neue Funktionen eingeführt. Wer Updates ignoriert, nimmt in Kauf, dass Programme nicht richtig funktionieren, lässt sich neue Funktionen und Verbesserungen entgehen – und läuft Gefahr Opfer von Kriminellen zu werden. Sicherheits-Updates, Bug-Fixes oder Patches sind dabei hervorzuheben, denn sie kümmern sich um Schwachstellen in der Software und sollten daher möglichst schnell installiert werden.

2. Malware, also Schadsoftware, verbreitet sich über E-Mail-Anhänge, manipulierte Links oder vermeintlich sichere Downloads. Zwar ist auch eine Übertragung über beispielsweise einen USB-Stick möglich, die meisten Angriffe geschehen jedoch online. Malware kann viele Formen annehmen: Computervirus, Trojaner, Ransomware oder Spyware sind nur einige der vorhandenen Arten.

3. Social Engineering beschreibt einen Oberbegriff für viele verschiedene Arten von Betrug und Täuschung: Telefon- oder E-Mail-Betrug mit Datenabfragen und unseriösen E-Mail-Anhängen. Phishing ist dabei die häufigste

Online-Methode. Ziel von Phishing-Versuchen ist es meistens sensible Informationen zu erhalten – Login-Daten zu Websites, Kreditkartennummern oder Zugänge zum Onlinebanking.

4. Der Begriff Doxxing kommt vom Englischen „docs", also „documents". Beim Doxxing werden entsprechend persönliche Dokumente und Daten gesammelt und im Internet veröffentlicht. Das können private Adressen und Telefonnummern sein, Scans von Ausweisdokumenten, Bankdaten, aber auch ganze E-Mail-Nachrichtenverläufe oder Screenshots von Messenger-Chats. Betroffen sind oft Personen des öffentlichen Lebens, etwa Politiker:innen.

5. Beim Identitätsdiebstahl gibt sich eine Person im Internet für eine andere aus. Kriminelle nutzen dafür zum Beispiel persönliche Daten, die sie im Internet gefunden oder erbeutet haben. Woher sie diese erhalten haben, bleibt meist unklar. Sie können aus erfolgreichen Phishing-Versuchen, Datenlecks bei großen Online-Plattformen oder aus öffentlich einsehbaren Informationen stammen. Identitätsdiebstahl zielt häufig auf Geld ab: Betrüger:innen richten auf fremden Namen Nutzerkonten ein und bestellen Waren oder Dienstleistungen oder schließen kostenpflichtige Abos ab.

6. Bei einem Scam handelt es sich übergreifend um Betrug, bei dem durch Täuschung versucht wird an Informationen oder Geld zu gelangen. Scams können ganz unterschiedlicher Form sein, eine weit verbreitete Methode ist jedoch der sogenannte Vorschussbetrug. Anzeichen einer Fälschung können beispielsweise kleine Fehler und Ungenauigkeiten bei E-Mail-Adressen oder Absendern sein.

Flexibles Weiterbildungsangebot stärkt auch berufliche Möglichkeiten

Sich sicherer im Umgang mit digitalen Tools und dem Internet zu fühlen ist für viele Verbraucher:innen ein Hauptgrund, um sich weiterzubilden. Denn die Stärkung digitaler Kompetenzen ermöglicht Verbraucher:innen eine selbstbestimmte Nutzung aktueller digitaler Dienste. Doch auch im digitalen Berufsalltag wird es immer wichtiger sich auszukennen. Entsprechendes Wissen und Fähigkeiten bieten auch auf dem Arbeitsmarkt entscheidende Vorteile.

Viele Unternehmen sind heutzutage auf der Suche nach Auszubildenden oder Mitarbeitenden, die über digitale Grundkenntnisse verfügen, da ihre modernen Systeme dies schlichtweg verlangen. Mit der Komplexität der Systeme steigen auch die Sicherheitsrisiken. Eine Möglichkeit sich bezüglich derartiger Kenntnisse rückzuversichern, wird für Arbeitgeber entsprechend immer wichtiger. Die Zertifizierungsmöglichkeit des Digitalführerscheins sorgt dafür, dass der Stand der eigenen digitalen Kompetenz nicht nur aufgezeigt, sondern auch für Dritte wie beispielsweise Arbeitgeber einheitlich nachvollziehbar gemacht wird, denn Bewerber:innen und Mitarbeiter:innen können ihre Kenntnisse beim Arbeitgeber transparent verdeutlichen.

Die geplante Erweiterung des Lernangebots um spezifische Fokusthemen, die auf spezielle Themengebiete wie Computersprache eingehen oder sich an einzelne Berufsgruppen wie beispielsweise pädagogische Fachkräfte richten, verstärkt die Bedeutung des Digitalführerscheins im beruflichen Kontext weiter.

Ergänzendes Newsportal mit aktuellen Updates zu Digitalthemen

Mit „DiFü-News" verfügt der Digitalführerschein zusätzlich über einen aktuellen Newsbereich rund um relevante Themen aus dem digitalen Alltag. Die Artikel können den sechs übergreifenden Themenbereichen des Lernangebots zugeordnet werden und unterstützen so die Wissensvermittlung in Bereichen wie Gefahrenschutz, Datenwelt oder Technologiealltag. Der zugehörige Podcast „D wie Digital" ergänzt das Angebot dabei auf auditiver Ebene. Orientiert an den Themenbereichen des Lernangebots und am aktuellen News-Geschehen werden entsprechende Themen wie Ransomware, Algorithmen oder digitale Selbstverteidigung gemeinsam mit wechselnden Expert:innen besprochen und aktuelle Ereignisse eingeordnet.

IT-Sicherheit im Mittelstand

Es stehen jedoch nicht nur Einzelpersonen vor der Herausforderung digitale Sicherheit in ihr privates sowie vor allem das berufliche Leben zu integrieren. Auch viele kleine und mittlere Unternehmen (KMU) oder Handwerksbetriebe müssen sich mit IT-Sicherheit auseinandersetzen. Besonders für Unternehmen ist es dabei wichtig aus einer Vielzahl bestehender Angebote die passenden für ihre IT-Sicherheit zu finden und umzusetzen. Viele Maßnahmen zur Verbesserung der IT-Sicherheit sind auch ohne große Investitionen im Mittelstand umsetzbar. Es bedarf jedoch klarer Strukturen und Abläufe, um das IT-Sicherheitsniveau nachhaltig zu erhöhen. Zunächst sollte beispielsweise ein umfassendes Sicherheitsverständnis der Belegschaft entwickelt und gefördert werden. So kann der Faktor Mensch als Einfallstor für Cyberkriminelle bereits reduziert werden. Weitere Vorkehrungen sollten zum Beispiel regelmäßige Updates der Systeme und die Erstellung von Sicherungskopien beinhalten. Vor allem kleinere Betriebe, die in der Regel über keine eigene IT-Abteilung verfügen, können ihren Grundschutz

bereits durch derartige, kleine Vorsichtsmaßnahmen deutlich erhöhen. Mit dem durch die Transferstelle IT-Sicherheit im Mittelstand (TISiM) entwickelten onlinebasierten Tool, dem Sec-O-Mat, können Unternehmen, Freiberufliche und Handwerksbetriebe nach einer kurzen Unternehmensbefragung bedarfsgerechte Umsetzungsvorschläge zur Verbesserung der IT-Sicherheit erhalten. Der im Anschluss an die Befragung ausgespielte TISiM-Aktionsplan enthält am Bedarf des Unternehmens orientierte Umsetzungsvorschläge. Regionale Anlaufstellen bei IHKs und an weiteren Standorten, sowie das TISiM-Mobil sorgen zudem dafür, dass Unternehmen auf ihrem Weg zu mehr IT-Sicherheit auch vor Ort begleitet werden. So gelangt das Wissen von Experten und Expertinnen zielgerichtet dorthin, wo es benötigt, wird: in die Unternehmen.

Doch nicht nur das TISiM-Mobil sorgt für Support: Auch der Digitale Engel als weitere Initiative von Deutschland sicher im Netz e.V. bietet mit seinem Mobil bundesweit Hilfestellungen für ältere Menschen & Multiplikator:innen in der Seniorenarbeit an, während Projekte wie Digitale Bildung macht Schule (DigiBitS) sich direkt an Lehrkräfte und Schüler:innen richten.

Der Digitalführerschein als deutschlandweites Weiterbildungsangebot

Einblicke in die Funktionsweisen von Hard- und Software, Souveränes Erkennen von Falschinformationen, die Zuordnung von Gefahren und das Wissen über die Mittel, um sich zu schützen: Ob im beruflichen oder privaten Kontext, die Vermittlung von digitalen Kompetenzen sorgt für einen sichereren und selbstbestimmten Umgang mit den aktuellen digitalen Entwicklungen und Möglichkeiten. Der DsiN-Digitalführerschein als deutschlandweites Weiterbildungsangebot macht Jung und Alt fit fürs Netz und den digitalen Raum für alle zugänglich.

Über den Autor

Dr. Michael Littger
ist seit 2013 Geschäftsführer der Initiative „Deutschland sicher im Netz“. Davor leitete er das Kompetenzfeld Digitale Wirtschaft, Telekommunikation, Medien beim Bundesverband der Deutschen Industrie (BDI).

DsiN Deutschland sicher im Netz

DER DSIN-DIGITALFÜHRERSCHEIN IM ÜBERBLICK

6 Themen, 6 Teilprüfungen

Die Prüfung zum DsiN-Digitalführerschein (DiFü) besteht aus sechs Teilprüfungen. Jede Teilprüfung enthält Fragen zu den sechs Themenbereichen Geräte, Internet, Kommunikation, Datenwelt, Gefahrenschutz und Technologiealltag.

Dauer der Prüfung

Pro Teilprüfung gibt es 10 Minuten Zeit, für die Gesamtprüfung 60 Minuten. Ist die Zeit um, bleiben noch offene Fragen unberücksichtigt, auch wenn sie noch beantwortet werden können.

Prüfung bestanden

Die Prüfung ist bestanden, wenn mindestens 50 Prozent der Fragen richtig beantwortet sind, pro Teilprüfung müssen fünf Antworten richtig sein. Die Gesamtprüfung gilt nur dann als bestanden, wenn alle Teilprüfungen erfolgreich absolviert wurden.

Durchgefallen?

Wer den DsiN-DiFü nicht auf Anhieb schafft kann die Prüfung so oft wie gewünscht wiederholen. Bestandene Teilprüfungen behalten ihre Gültigkeit und müssen nicht wiederholt werden.

Das Zertifikat

Nach bestandener Prüfung fügt die Initiative Name und Geburtsdatum ein, der „Digital-Führerschein“ kann dann direkt heruntergeladen und in den sozialen Netzwerken geteilt werden.

Hier geht es direkt zum DsiN-DiFü:

Prof. Dr. Alexander Roßnagel, Jürgen Hartz und Prof. Dr. Dieter Kugelmann auf dem 1. Datenschutztag Hessen & Rheinland-Pfalz in Frankfurt am Main.

"WER DATENSCHUTZ NEBENBEI MACHEN SOLL, IST SCHNELL ÜBERLASTET"

Zum 1. Datenschutztag Hessen & Rheinland-Pfalz für behördliche und kommunale Datenschutzbeauftragte hatten die Landesbeauftragten für den Datenschutz und die Informationsfreiheit aus Rheinland-Pfalz und Hessen gemeinsam mit dem Berufsverband der Datenschutzbeauftragten Deutschland (BvD) e.V in Frankfurt am Main eingeladen. Über die Herausforderungen für kommunale und behördliche Datenschutzbeauftragte und das Angebot der Aufsichtsbehörden sprachen die BvD-News mit dem Hessischen Landesbeauftragten für Datenschutz und Informationsfreiheit, **Prof. Dr. Alexander Roßnagel**, seinem rheinland-pfälzischen Amtskollegen **Prof. Dr. Dieter Kugelmann** und BvD-Vorstandsmitglied **Jürgen Hartz**.

Ein Interview über die Herausforderungen für behördliche und kommunale Datenschutzbeauftragte und den 1. Datenschutztag Hessen & Rheinland-Pfalz.

BvD-News: *Wie kam es überhaupt zu der Idee einen eigenen Behördentag in Frankfurt am Main ins Leben zu rufen?*

Jürgen Hartz: Wir sehen schon seit geraumer Zeit, dass die Datenschutzbeauftragten in Behörden und kommunalen Verwaltungen ganz eigene Fragen haben, dabei oft aber alleine stehen. Dies wollten wir angehen. Und die Mitte in Deutschland schien uns dafür ein geeigneter Ort zu sein, um vielen die Anreise und Teilnahme zu erleichtern. Der Tag ist übrigens nicht nur für Datenschutzbeauftragte in den Kommunen und Verwaltungen von Hessen und Rheinland-Pfalz interessant, sondern für Datenschutzbeauftragte aus ganz Deutschland.

Alexander Roßnagel: Wir hatten schon seit längerem mit dem BvD darüber gesprochen, dass ein solcher Tag zentral mitten in Deutschland interessant wäre. Als wir dann jemanden dazu holen wollten, war Rheinland-Pfalz unsere erste Wahl.

Dieter Kugelmann: Als beide Organisationen auf mich zukamen, habe ich sofort zugesagt. Und zwar aus zwei Gründen: Zum einen machen wir für die Zielgruppe der behördlichen und kommunalen Datenschutzbeauftragten in den verschiedenen Regionen von Rheinland-Pfalz bereits viele Veranstaltungen. Diesen Ansatz überregional weiterzuverfolgen mit dem BvD und den hessischen Kolleginnen und Kollegen fanden wir reizvoll. Zum anderen konnten wir den Austausch zwischen unseren Aufsichtsbehörden auf diese Weise intensivieren. Wir arbeiten ja schon seit Jahren eng zusammen. Das nach außen sichtbar zu machen, war einfach eine gute Idee.

BvD-News: *Welche Herausforderungen stellen sich speziell für Datenschutzbeauftragte in der Verwaltung?*

Dieter Kugelmann: Wir haben vor einiger Zeit im Rahmen eines Kommunalprojekts in den Kommunen von Rheinland-Pfalz

erhoben, wie die Stimmung unter den dortigen Datenschutzbeauftragten ist. Eines der Ergebnisse war, dass viele von ihnen nur nebenbei, manchmal mit nur fünf Prozent ihrer Arbeitszeit, den Datenschutz im Hause koordinieren sollen. Aufgrund des durch die Datenschutz-Grundverordnung bedingten Zuwachses an Aufgaben der Datenschutzbeauftragten empfehlen wir je nach Größe der Verwaltung einen Personalbedarf in Höhe von 30 bis 50 Prozent einer Vollzeitstelle. Das aber löst bei vielen Kommunen sofort Ängste aus, der Landesrechnungshof könnte dies beanstanden. Wir haben dann mit dem Rechnungshof gesprochen und eine Lösung gefunden. Aber mit mancher Kommune bleibt es schwierig.

Alexander Roßnagel: Dabei fallen gerade in den Kommunen, beispielsweise bei der Polizei, sehr viele Daten an. Wer dann nur nebenbei Datenschutz machen soll, ist schnell überlastet. Und in kleineren Gemeinden passiert es nach wie vor, dass jemand einfach zum Datenschutzbeauftragten ernannt wird, die Person aber überhaupt nicht weiß, was sie machen soll. Wo kriegt sie Informationen her? Wo gibt es Weiterbildungen, Checklisten, Hilfen, Gesetzesverweise? Eine Ausbildung gibt es für behördliche Datenschutzbeauftragte nicht. Und Weiterbildungen muss der Dienstherr genehmigen. Der Bedarf dafür wird aber nicht immer bei der Hausspitze gesehen.

Jürgen Hartz: Als Berufsverband der Datenschutzbeauftragten Deutschlands sehen wir es auch deshalb als unsere Aufgabe an diese Gruppe zu stärken, Hilfsmittel bereit zu stellen und eben mit dieser Veranstaltung sie bei ihren Fragen zu unterstützen. Denn oft stehen die Datenschutzbeauftragten in Kommunen und Ämtern wirklich auf verlorenem Posten. Da sind Beratung, der Austausch und das Netzwerken besonders wichtig.

BvD-News: *Welche Themen standen im Mittelpunkt dieser ersten Veranstaltung in Frankfurt?*

Dieter Kugelmann: Unter anderem ging es um die Öffentlichkeitsarbeit etwa über Social-Media-Kanäle der Kommunen, die Digitalisierung in der Verwaltung spielte eine große Rolle, auch die Anwendung von Künstlicher Intelligenz in Behörden und Ämtern.

Alexander Roßnagel: Uns war wichtig, die drängendsten Fragen der Datenschutzbeauftragten in Behörden und Kommunen aufzugreifen, und als Aufsichtsbehörden Antworten zu geben. Daneben war der Austausch gerade länderübergreifend zwischen den Datenschutzbeauftragten in den Verwaltungen besonders wichtig. Zu sehen, dass sie womöglich mit ähnlichen Problemen konfrontiert sind, aber eine Seite vielleicht schon etwas weiter ist, das hat sicher manchem geholfen, genauso wie die Best-Practice-Beispiele, die in den Vorträgen und Diskussionen genannt wurden.

BvD-News: *Welche Rolle spielte die Begegnung mit den Aufsichtsbehörden für die Datenschutzbeauftragten?*

Jürgen Hartz: Wir machen oft die Erfahrung, dass Datenschutzbeauftragte anfangs befürchten im Gespräch mit den Aufsichtsbehörden etwaige Schwachstellen preis zu geben. Aber wenn sie sich dann doch trauen, erleben sie, wie kooperativ und unterstützend die Aufsichtsbehörden sind. Das ist eine wichtige Erfahrung, die die Arbeit der Datenschutzbeauftragten nachhaltig verändert. Und das haben wir in Frankfurt auch wieder erlebt.

Dieter Kugelmann: Wir ermutigen die Datenschutzbeauftragten ausdrücklich mit uns ins Gespräch zu kommen. Diese Gelegenheit haben in der Vergangenheit manche und während der Veranstaltung viele genutzt. Wenn das Bestehen dieser Möglichkeit an die Verantwortlichen weitergegeben wird und wir durch Unterstützung datenschutzgerechte Lösungen herbeiführen können, dann ist das ein großer Erfolg der Veranstaltung.

Alexander Roßnagel: Ich hatte auch den Eindruck gewonnen, dass Einige mit durchgedrücktem Kreuz nachhause gefahren sind und sich vorgenommen haben sich mehr zu trauen oder durchzusetzen.

BvD-News: *Welches Fazit ziehen Sie aus diesem ersten Datenschutztag Hessen & Rheinland-Pfalz?*

Dieter Kugelmann: Ich glaube, dass wir mit den Themen und der Mischung aus Vorträgen und Workshops genau die Fragen der Teilnehmenden getroffen haben. Denn nicht alle Verwaltungen halten sich beim Datenschutz an die Gesetze. Da sind Hinweise, Tipps, Hilfen und immer wieder der Austausch wirklich hilfreich und ermutigend.

Alexander Roßnagel: Wir haben zudem in der Schlussrunde, in der wir als Aufsichtsbehörden die Fragen der Teilnehmenden beantworteten, die Spannbreite der Themen erlebt, die behördliche und kommunale Datenschutzbeauftragte umtreibt. Da waren tiefergehende Fachfragen ebenso dabei wie Fragen nach einer Strategie, um zum Beispiel die Behörde davon zu überzeugen, dass die Nutzung von in den USA gehosteten Videoplattformen gegen Gesetz verstößt. Diese Offenheit hat mich sehr beeindruckt.

Jürgen Hartz: Mich hat begeistert, dass wir unsere Zielgruppe der behördlichen und kommunalen Datenschutzbeauftragten wirklich erreicht haben. Als ich vom Podium herunterblickte, habe ich so viele neue Gesichter gesehen. Das freut uns als BvD natürlich sehr. Denn wir verstehen uns auch für sie als Ansprechpartner und Interessenvertretung. Von daher würde ich sagen: Wir sehen uns in einem Jahr wieder.

CHRISTINA DENZ

KRITISCHE STIMMEN IM GLITTERREGEN

Bei der DAME-Preisverleihung holten ein Künstlerkollektiv, zwei Journalisten und ein Schülerprojekt die Trophäen für 2021.

Nach zwei Jahren Corona konnten die Preisträger des Datenschutz Medienpreises DAME ihre Trophäen endlich wieder persönlich auf den Verbandstagen 2022 in Berlin entgegennehmen. Vier Beiträge hielt die Jury aus Datenschutz- und Kulturexperten in diesem Jahr für preiswürdig. Alle Beiträge überzeugten nicht zuletzt durch lange Recherche und eine professionelle Produktion.

„Made to Measure" gewinnt Hauptpreis

Hans Block nahm für die Künstlergruppe Laokoon den mit 3.000 Euro dotierten DAME-Hauptpreis entgegen.

Den mit 3.000 Euro dotierten Hauptpreis erhielt das Künstlerkollektiv Laokoon für ihr filmisch erzähltes Experiment „Made to Measure - eine digitale Spurensuche" über die Rekonstruktion einer Person anhand anonymisierter Daten. Dazu hatten die drei Künstler und Filmemacher Moritz Riesewieck, Hans Block und Cosima Terrasse Interessierte europaweit aufgerufen der Gruppe anonymisierte Daten zur Verfügung zu stellen. Über 100 Personen folgten dem Aufruf, die Künstlergruppe wählte daraus einen Datensatz aus. Eine Schauspielerin begann dann sich ausschließlich aufgrund dieser Informationen mit Frisur, Gestik, Job und privaten Interessen der Person hinter den Daten anzunähern.

Zwei Jahre arbeitete das Kollektiv, das sich mit seinem Namen an die berühmte Skulptur der Laokoon-Gruppe aus römischer Zeit anlehnt, an dem Projekt, unterstützt von der Kulturstiftung des Bundes und dem WDR. Bekannt wurden Block und Riesewieck bereits mit dem vielfach ausgezeichneten Dokumentarfilm „The Cleaners" über junge Menschen in Asien, die für Social-Media-Plattformen Beiträge und Videos mit Gewaltdarstellungen, Pornografie oder Hassreden herausfiltern.

Hans Block
von der Künstlergruppe Laokoon:

Wir interessieren uns sehr für Themen rund um die Digitalisierung, wollen aber hinter die glänzende Oberfläche schauen. Daher kommt unser Name: Laokoon erkannte der Sage nach als einziger im hölzernen Pferd der Trojaner einen Betrug, weil er eben hinter die Kulisse des vermeintlichen Geschenks gesehen hatte. Wir nutzen die Form der Dokumentation, um unsere Themen künstlerisch zu verarbeiten und damit den öfffentlichen Raum, der sich ja auch im Digitalen zeigt, gesellschaftspolitisch umzudeuten.

Carsten Damm
vom Kinder- und Jugendpfarramt der Evangelischen Landeskirche Anhalts:

Wir verstehen unsere Arbeit als Mehrgenerationenprojekt, an dem die Schauspielerinnen und Schauspieler im Teenageralter, ich als angehender Medienpädagoge und mein Vater, der das Projekt vor 13 Jahren zum ersten Mal initiiert hatte, zusammenarbeiten. Als wir begonnen haben, hatte ich selbst noch als Schüler mitgespielt. Mittlerweile entstehen die Stücke, die wir drehen, in einem einwöchigen Workshop, bei dem die Schülerinnen und Schüler mit uns ein Thema und ein Skript entwickeln und wir es dann gemeinsam realisieren.

Jeweils 1.500 Euro Preisgeld holten bei der DAME 2021 das Schüler-Videoprojekt „schreibt …“, eine Vater-Sohn-Kolaboration von Carsten Damm und Hans Höpfner aus Dessau, die Print-Reportage „Mein Gesichtsverlust“ von „Spiegel“-Autor Patrick Beuth über das US-Startup Clearview sowie das Radio-Feature „Drei Jahre DSGVO - Was hat die EU-Verordnung zum Datenschutz gebracht?“, in dem Tobias Dirr erzählt, welche Auswirkungen die DSGVO auf die Website seiner Band hatte.

Tobias Dirr
freier Journalist:

Als freier Autor habe ich mich vorher bereits mit dem Thema Datenschutz beschäftigt. Über die DSGVO wurde ja viel berichtet, vor allem zum Start. Aber welche Auswirkungen die Regeln auf kleinere Unternehmen, Vereine oder eben auch meine Band haben, das hat mich interessiert. Ich habe mich also auf die Suche gemacht nach Menschen, die mir erklären können, was man berücksichtigen muss, wenn man eine Website veröffentlicht. Denn unsere Band-Homepage hatten wir zunächst offline geschaltet, weil wir nicht mehr wussten, was richtig und was falsch ist.

Jury-Mitglied und YouTuber Eric Hohenadel, Jugendjuror der Initiative klicksafe, freute sich vor allem darüber, dass von den insgesamt 39 eingereichten Beiträgen viele explizit junge Leute ansprachen. Und dennoch seien viele der Bewerbungsarbeiten geeignet alle Altergruppen für das Thema Datenschutz zu gewinnen, sagte BvD-Vorstandsvorsitzender Thomas Spaeing zum Auftakt der Preisverleihung.

Patrick Beuth
Autor bei „Der Spiegel“:

Nachdem die „New York Times“ über das fragwürdige Geschäftsmodell von Clearview AI geschrieben hatte, war mir schnell klar, dass auch deutsche und europäische Staatsbürger:innen in die Biometrie-Datenbank des Unternehmens gelandet sein müssen. Ich selbst zum Beispiel. Und so entstand die Idee, der Firma auf den Zahn zu fühlen und gleichzeitig zu recherchieren, wie es überhaupt soweit kommen konnte, dass sich heute kaum noch jemand vor so etwas verstecken kann. Das größte Hindernis war dabei die schleppende Kommunikation mit Clearview. Die Antworten dauerten wochenlang, ich musste zwischendrin mit einer Datenschutzbeschwerde drohen. Das immerhin hat geholfen. Als Reaktion auf meine Rechercheergebnisse habe ich versucht, Fotos von mir aus dem Netz löschen zu lassen, was aber nur in Teilen funktioniert hat. Mein Standardfoto habe ich verfremdet, und ich achte seither noch mehr darauf, keine weiteren Gesichtsfotos von mir (und anderen) im Netz zu veröffentlichen.

DAME-Preisverleihung auf den BvD-Verbandstagen im Mai 2022 in Berlin

Svea Eckert, die im vergangenen Jahr mit Henning Wirtz den Hauptpreis holte, war begeistert, dass alle Einreichungen „keineswegs langweilig“ waren. Traditionell sind die Gewinner des Hauptpreises in der nachfolgenden Ausschreibung Mitglied der Jury. Dieser gehörten wieder die Landesbeauftragte für den Datenschutz Niedersachsen, Barbara Thiel, der Vorstand der Stiftung Datenschutz, Frederick Richter, Dr. Sebastian Sprenger und Tobias Meinsel von der DATEV-Stiftung Zukunft, Marion Zinkeler, Vorständin der Verbraucherzentrale Bayern sowie Stefanie Rack vom EU-Projekt klicksafe an. Neu dabei war Wolfgang Stückemann, Vorstandsvorsitzender des Deutschen Spendenrats.

Barbara Thiel zeigte sich begeistert: „Jeder Wettbewerb war bislang anders“, sagte sie nach der Preisverleihung. „Deshalb wollen wir unbedingt weitermachen.“

Der Datenschutz Medienpreis DAME wird seit November 2018 von der DATEV-Stiftung Zukunft gefördert. Medienpartner ist die Medienkompetenzinitiative klicksafe.

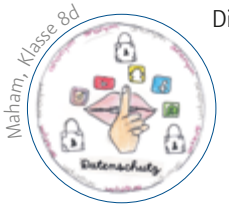
Über die Autorin

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

▶ www.datenschutzmedienpreis.de

JUNGE TALENTE MIT KREATIVEN IDEEN FÜR DATENSCHUTZ AUSGEZEICHNET

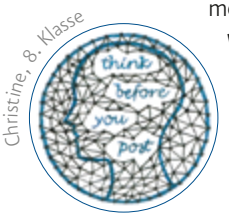
175 Motive haben Schüler:innen und Klassen für den Kreativwettbewerb der BvD-Initiative „Datenschutz geht zur Schule“ (DSgzS) eingereicht, sechs davon werden jetzt als Aufkleber produziert.



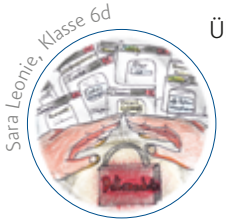
Maham, Klasse 8d

Hedwig, 9. Klasse

Johanna, 8. Klasse



Christine, 8. Klasse


Sara Leonie, Klasse 6d

Die Idee für Aufkleber als neue Give Aways für die BvD-Initiative „Datenschutz geht zur Schule“ (DSgzS) entstand bei der Neuproduktion der begehrten Webcam-Sticker, die die Initiative bereits in den Schulen verteilt. Von Januar bis Ende April 2022 konnten sich Schüler:innen und Klassen mit selbstgestalteten Motiven für Aufkleber zum Datenschutz bewerben.

175 gemalte oder gezeichnete Bilder von 38 einzelnen Schüler:innen und 13 Schulklassen gingen für den Wettbewerb ein. Der Arbeitskreis Schule (AK Schule) traf eine Vorauswahl, die Jury, der die TV-Moderatoren Steven Gätjen und Shary Reeves, der Informatik-YouTuber Cedric Mössner mit seinen „Morpheus Tutorials“, die als TotallyGamerGirl bekannte Christine Links und Werner Fütterer aus dem Vorstand des Bunds der Kunsterziehenden angehörten, wählten die Gewinnerinnen. Sie wurden am 21. Juni auf einer Online-Preisverleihung bekannt gegeben.

Über Sachpreise können sich Christine aus Weiden und Johanna aus Wiesbaden freuen, die jeweils in die 8. Klasse gehen. Auch Hedwig aus einer 9. Klasse in Görlitz gehört zu den Siegerinnen.

Der mit 300 Euro dotierte Klassenpreis ging an den Kunstkurs einer 11. Klasse in Meppen sowie an eine 6. und 8. Klasse einer Schule in Groß-Gerau. Von dort kamen besonders viele Einreichungen. Den Grund dafür nannte Lehrerin Birgit Marheinecke bei der Online-Siegerehrung: „Datenschutz ist bei uns festes Thema in allen 5. Klassen. Schüler:innen aus den 11. Klassen kommen als Mentoren und schulen die Jüngeren.“

Romina, Kunstkurs 11. Klasse

AK-Schule-Vize-Sprecher Frank Spaeing betonte zuvor bei der Online-Veranstaltung: „Unser Leben ist digital, wer weiß das besser als ihr. Aber das digitale Leben funktioniert nicht ohne Datenschutz.“ YouTuber und Informatik-Dozent Mössner warb unter anderem für Passwortmanager und Zwei-Faktor-Authentifizierung und warnte vor kostenlosen Downloads aus dem Internet. *dhe*

Die Motive der Schülerinnen werden jetzt mit dem DSgzS-Logo kombiniert und nach einem grafischen Feinschliff als Aufkleber in die Produktion gegeben. Schulklassen können die Sticker über die BvD-Geschäftsstelle bestellen. Die prämierten Motive sind online abrufbar auf:

▶ https://www.bvdnet.de/kreativpreis/

DOZENT:INNEN GESUCHT

Wer als Dozent:in bei DSgzS aktiv werden möchte, ist herzlich willkommen sich bei der Initiative zu melden! Alle Infos auf: www.dsgzs.de

LINK-TIPP

Data Protecion and Privacy Legislation Worldwide

Überblick und aktuelle Daten über neue und anhängige Datenschutzgesetze, die in Kraft treten.

▶ https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

GDPR Enforcement Tracker

Der CMS.Law GDPR Enforcement Tracker ist eine Übersicht über Bußgelder und Strafen, die Datenschutzaufsichtsbehörden innerhalb der EU im Rahmen der DSGVO verhängt haben. Da nicht alle Bußgelder veröffentlicht werden, kann die Übersicht natürlich nie vollständig sein, weshalb jeder Hinweis auf weitere DSGVO-Bußgelder und -Strafen gerne aufgenommen wird.

▶ https://www.enforcementtracker.com/

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

JUBILÄUM BEIM DATENZIRKUS

BvD-Blogreihe von Rudi Kramer und Frank Spaeing feiert 40. Ausgabe

Es tut sich sehr viel in der Rechtsentwicklung, sei es durch Verlautbarungen der Aufsichtsbehörden, sei es durch Rechtsprechung, Aktivitäten des Gesetzgebers, Veröffentlichungen von kompetenten Einrichtungen und Kanzleien oder auch durch gesellschaftliche Diskussionen rund um Datenverarbeitung. Da fällt es manchmal schwer den Überblick zu behalten.

Um seinen Mitgliedern zu unterstützen, hat der BvD vor über einem Jahr eine Blogreihe ins Leben gerufen: „Menschen, Daten, Sensationen – Rudis Bericht aus dem Datenzirkus, ergänzt um Franks Zugabe“. Am 4. Juni 2022 ist die 40. Ausgabe erschienen.

Zu verdanken ist die breite Palette mit News dem ehrenamtlichen Engagement von Rudi Kramer und Frank Spaeing, die stets Neuigkeiten aus verschiedensten Veröffentlichungen screenen und fast wöchentlich zusammenstellen. Neben fachlichen Themen aus den Bereichen Aufsichtsbehörden, Rechtsprechung, Gesetzgebung, Veröffentlichungen und gesellschaftliche Diskussionen gibt es immer wieder einen „Blick über den Tellerrand“. Kaum verwunderlich vor dem Hintergrund, dass sich beide Autoren auch für die Initiative „Datenschutz geht zur Schule“ einsetzen. Mittlerweile ist das Themenspektrum des Blogs ergänzt um „Ethik und Künstliche Intelligenz“ und erhält durch den Nachtrag von Frank Spaeing noch Aufwertung durch speziell IT-spezifische und bürgerrechtliche Aspekte.

Nach über einem Jahr lässt sich die Blogreihe von Kramer und Spaeing mit Fug und Recht als Erfolgsstory bezeichnen: Die Aufrufzahlen und das positive Feedback vieler BvD-Mitglieder zeigen, dass dieser Informationsservice gut angenommen wird. Und nicht mehr und nicht weniger möchte er sein. „Ziel unserer Blogreihe ist es die Leserschaft auf interessante Neuigkeiten hinzuweisen“, sagen die Autoren. „Die vertiefe Auseinandersetzung bleibt dann denjenigen überlassen, die das jeweilige Thema gerade aktuell bearbeiten.“ Und sie fügen hinzu: „Das Ganze wäre nicht möglich ohne die vielen Quellen und die vielen aktiven Zeitgenoss:innen, die ihrerseits Quellen und Einschätzungen teilen.“

Wer keine Ausgabe der Blogreihe „Menschen, Daten, Sensationen“ verpassen möchte kann den BvD-Blog als RSS-Feed auf der BvD-Website abonnieren unter:

▶ https://www.bvdnet.de/feed/

INTERNATIONALES IN DER REGIONALGRUPPE FRANKFURT

Rund 25 Teilnehmende diskutiert über den internationalen Datenaustausch und die Vorhaben der EU.

Dr. Christoph Ritzer, Partner der Kanzlei Norton Rose Fulbright, erläuterte auf dem Treffen der BvD-Regionalgruppe Frankfurt am Main die derzeitigen Datenschutz-Vorhaben der EU.

Mit zwei Gastbeiträgen ist die Regionalgruppe Frankfurt des BvD am 28. Juni wieder in das erste Präsenztreffen nach der Corona-Pandemie gestartet. Eingeladen waren der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Alexander Roßnagel, und Dr. Christoph Ritzer, Partner der internationalen Wirtschaftskanzlei Norton Rose Fulbright.

Alexander Roßnagel, der zuvor mit seinem rheinland-pfälzischen Amtskollegen Prof. Dr. Dieter Kugelmann und dem BvD den ersten Datenschutztag Hessen & Rheinland-Pfalz für behördliche und kommunale Datenschutzbeauftragte durchgeführt hatte, skizzierte seine Perspektive auf mögliche Lösungsversuche der EU-Kommission zum Datenaustausch mit den USA am Beispiel von Videokonferenzanbieter wie Zoom, Microsoft Teams und Webex. Dabei zeigte sich Roßnagel überzeugt, dass die von der EU geplante neue Einigung mit den USA vor dem EuGH wieder keinen Bestand haben wird.

Denn neben der erwarteten neuerlichen Klage des österreichischen Daten-Aktivisten Max Schrems vor dem EuGH könnten auch die Aufsichtsbehörden den Klageweg beschreiten: Und zwar über die Verwaltungsgerichte bis hin zum Bundesverwaltungsgericht, um den möglichen Datentransfer aus Europa zu US-Servern etwa über die Videosysteme in Ämtern und Behörden zu unterbinden.

Christoph Ritzer gab einen Überblick zum aktuellen Stand der geplanten EU-Regularien Digital Markets Act, Digital Services Act, Data Act, Data Governance Act und AI Regulations – und damit wie Alexander Roßnagel viel Stoff für Fragen und Diskussionen unter den rund 25 Teilnehmenden, die aus der Rhein-Main-Region zum Regionalgruppentreffen gekommen waren.

Gruppen-Sprecherin Caroline Böhm und Kollege Dr. Christoph Bausewein freuten sich, dass das Treffen wieder in Präsenz und mit intensivem Austausch stattfinden konnte. „Nun sehen wir uns wieder ganz“, sagte Caroline Böhm zum Auftakt. „Die vergangenen Male konnten wir uns nur über die kleinen Kacheln der Videokonferenz und nur die Köpfe sehen.“ *chd*

Anzeige

PIA & ALFRIGHT

Die perfekte Kombi für alle Datenschutzbeauftragten

Hi, ich bin PIA.
Deine digitale Datenschutzbeauftragte.

Mit mir erledigst du deine Aufträge als Datenschutzbeauftragter in 75% weniger Zeit und betreust über 400 Kunden gleichzeitig!

Ich führe deine Kunden mit intuitiven **Online-Fragebögen** durch die Ersterhebung und alle weiteren Datenschutzaudits. Damit deine Kunden wissen, was als nächstens zu tun ist, ordne ich ihnen auch automatisiert **Aufgaben und Datenschutzmaßnahmen** zu.

Danach erstelle ich selbstständig die **gesamte DSGVO-Dokumentation** inklusive Verzeichnis von Verarbeitungstätigkeiten und Dokumentation der technischen und organisatorischen Maßnahmen.

Zudem sensibilisiere ich die Mitarbeiter deiner Kunden mit **12 innovativen Online-Trainings**. So kannst du mit mir ein **Umsatzplus** von über **€ 3.300 je Kunde** erzielen!

DSGVO APP

Hier erfährst du mehr über PIA: www.dsgvoapp.eu

Hi, ich bin ALFRIGHT.
Dein DSGVO Webseiten Butler.

Ich sorge dafür, dass die Webseiten deiner Kunden jederzeit datenschutz-konform & rechtssicher sind.

Ich analysiere **vollkommen selbstständig** die GESAMTE Webseite inklusive aller Unterseiten auf die Einhaltung rechtlicher Bestimmungen wie **DSGVO, BDSG, Eu-Cookie Richtlinie** und **TTDSG**.

Danach erhältst du von mir einen detaillierten **Bericht inklusive praxisorientierten Handlungsempfehlungen**, den du an deine Kunden weitergeben kannst. Zudem erstelle ich auf Basis des Tiefen-Scans auch eine passende Datenschutzerklärung.

Ich behalte für dich immer alles im Blick! Und damit mir auch nichts entgeht, **überwache** ich die Webseiten laufend. Natürlich halte ich auch die Datenschutz-erklärung stets aktuell.

ALFRIGHT

Hier erfährst du mehr über ALFRIGHT: www.alfright.eu

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE

Die wichtigsten Daten der BvD-Gremien

Detaillierte Informationen zu den Treffen und Terminen finden Sie unter:

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

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

08.09.2022	RG Gütersloh	**14.10.2022**	RG Stuttgart
21.09.2022	AK EVU	**21.10.2022**	RG Karlsruhe
23./24.09.2022	AK Externe	**21.10.2022**	RG München
26.09.2022	AK Schule	**21.11.2022**	AK Krypto
29.09.2022	RG Nord	**24.11.2022**	RG Nord
13.10.2022	RG Mitte	**01.12.2022**	RG Gütersloh

Bitte beachten Sie:

Aufgrund möglicher regionaler Corona-Beschränkungen bitten wir Sie sich vorab zu informieren, welche der Termine als Präsenztreffen und welche online stattfinden.

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

Termine und Anmeldung finden Sie auf unserer Webseite:

- www.bvdnet.de/termine/

BVD-STELLENBÖRSE

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

- www.bvdnet.de/bvd-stellenboerse

VERNETZEN SIE SICH MIT UNS:

- www.bvdnet.de

XING: www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

TWITTER: www.twitter.com/bvd_datenschutz

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

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

RSS-Feed: www.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 PRIVACY, SECURITY & GOVERNANCE

▶ www.onetrust.de

RHENUS OFFICE SYSTEMS

▶ www.rhenus.group/de

WEITERE WICHTIGE KONTAKTE

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

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

Marketing

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

Wettbewerb

Datenschutz Medienpreis 2022
Jetzt bewerben!
Einsendeschluss 05.12.2022
www.datenschutzmedienpreis.de
DAME 2022

Schulprojekt

"Datenschutz geht zur Schule" – DSgzS
Ein Projekt der Privacy4People gGmbH

Budapester Straße 31 · 10787 Berlin
Telefon (030) 26 36 77 58 · Telefax (030) 26 36 77 63
dsgzs@dsgzs.de · www.dsgzs.de

privacy4people

privacy4people - Gesellschaft zur Förderung des Datenschutzes gGmbH

IHRE SPENDE FÜR DEN DATENSCHUTZ:
Commerzbank
IBAN: DE 30 5054 0028 0424 5577 00
BIC: COBADEFFXXX

Telefon: +49 30 20 62 14 41
mail@privacy4people.de • www.privacy4people.de

HEIDELBERGER KOMMENTAR ZUM TTDSG

Prof. Dr. Rolf Schwartmann, Andreas Jaspers, Dr. Jens Eckhardt (Hrsg.)

Prof. Dr. Rolf Schwartmann, Andreas Jaspers, Dr. Jens Eckhardt (Hrsg.)
Heidelberger Kommentar: TTDSG Telekommunikations-Telemedien-Datenschutz-Gesetzt

C.F. MÜLLER

1. Auflage 2022-07-11
477 Seiten, Hardcover
119 Euro
ISBN 978-3-8114-5753-9

Mit ihrem Werk zum Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in der Reihe der Heidelberger Kommentare legen Schwartmann et al. den ersten großen Kommentar zur reichlich spät erfolgten Umsetzung der sog. ePrivacy-Richtline von 2002 (seit der Änderung 2009 auch als Cookie-Richtlinie bekannt) in das deutsche Recht vor.

Seit Dezember 2021 ist das TTDSG maßgeblich für die Ausgestaltung des Angebots von elektronischen Diensten und Medien, soweit der Datenschutz und die Integrität der zur Nutzung bzw. zum Abruf verwendeten Endgeräte betroffen sind. Dabei übernimmt das Gesetz zahlreiche Regelungsbereiche, die bisher nebeneinander im Telekommunikationsgesetz (TKG) sowie im Telemediengesetz (TMG) geregelt waren, insbesondere die Datenschutzbestimmungen.

Auf knapp 360 Seiten werden im vorliegenden Werk die 30 Paragraphen des TTDSG besprochen, weitere einhundert Seiten mit den – unkommentierten – relevanten Referenzen aus TKG, TMG, Netzwerkdurchsetzungsgesetz (NetzDG) und Medienstaatsvertrag (MStV) komplettieren das Nachschlagewerk. Die Inhalte des TTDSG werden ausnahmslos detailliert besprochen und sehr präzise eingeordnet. Dabei wird nicht nur die Historie inklusive der Änderungen im Gesetzgebungsverfahren umfassend dargestellt, es wird auch exakt zwischen den Regelungsbereichen abgegrenzt, die sich nicht oder nicht ausschließlich auf den Datenschutz beschränken. Auf naheliegende Denkfehler (etwa allein eine Interessenabwägung auf Basis von Art. 6 Abs. 1 lit. f DSGVO vorzunehmen) wird entsprechend hingewiesen. Die Inhalte – beispielsweise zur Entstehung der Regelungen – werden dabei auf die Aspekte beschränkt, die für die Auslegung und Anwendung der im Ergebnis vorliegenden Regelung relevant sind. Da das TTDSG in Teilen Regelungen aus TKG und TMG übernimmt, zahlt sich die Erfahrung des Autorenteams hier mehrfach aus.

An den nach wie vor bestehenden erheblichen Rechtsunsicherheiten, soweit das Gesetz eigene Standards, insbesondere beim Zugriff auf Endgeräte und die Regelung der entsprechenden Einwilligungen setzt, kann freilich auch Erfahrung nichts ändern. Die Autorinnen und Autoren begegnen dem wo immer möglich durch praxisgerechte Anregungen. So können beispielsweise Anbieter von TK- und Telemediendiensten wertvolle Hinweise zum korrekten Umgang mit Auskunftsverfahren finden. Wo sich noch keine Rechtsprechung herausgebildet hat, wird neben Analogien und der historischen Auslegung der Rechtstexte häufig mit Stellungnahmen von Aufsichtsbehörden gearbeitet, wobei wohltuend darauf ge-

achtet wird, diese als Rechtsauffassungen der Behörden darzustellen und nicht etwa als Regelung mit Gesetzeswirkung oder ausgeurteilter Rechtsprechung. Insoweit stellt der Kommentar immer eine belastbare Basis dar, auf die man Erwägungen bei der Umsetzung und Beachtung des TTDSG gut stützen kann. So ist der vorliegende Kommentar in jedem Fall hilfreich für die Praxis. Obwohl Unsicherheiten bei der Verwaltung von Cookies bleiben, ist allein die überzeugende Einbeziehung von Over-The-Top-Kommunikationsdiensten wie Messengern und Videokonferenzanbietern ins Fernmeldegeheimnis wertvoll, erübrigt sich doch häufig die Diskussion um Vereinbarungen zur Auftragsverarbeitung in Fällen, in denen die Bestimmung von Mitteln und Zwecken der Kommunikation seit jeher nicht eindeutig war. Eine Einordnung des Sanktionsregimes rundet das Werk ab, auch wenn die DSGVO-geplagte Leserschaft hier andere Bußgeldhöhen gewohnt ist.

Die angemessene Schwerpunktsetzung wird bereits aus den Seitenzahlen des Inhaltsverzeichnisses ersichtlich und dürfte die Interessen der meisten Leserinnen und Leser widerspiegeln. Während die Mehrzahl der Paragraphen drei bis zehn Seiten Platz in der Besprechung einnehmen, sind es für das Fernmeldegeheimnis (§ 3) sowie Störung und Missbrauch von Telekommunikationseinrichtungen und -diensten (§ 12) je gut 30 Seiten und für den prominenten § 25 über die Privatsphäre bei Endeinrichtungen knapp 50 Seiten.

Die Regelungen des § 25 TTDSG sind schließlich diejenigen, die auch in Zukunft Cookie bzw. Consent-Banner zum Teil jedes Besuches einer Webseite machen. Hier zeigt sich exemplarisch, dass die Autoren die vom Gesetzgeber offen gelassene Auslegung noch nicht grundsätzlich lösen können, aber die Regelung so umfassend beleuchten, dass die Leserschaft neben der „auf Nummer sicher gehenden" Lösung über Consent-Banner verschiedene Anregungen erhält, wie Betrugsprävention, bedarfsgerechte Gestaltung oder statistische Analysen ohne Nutzer-Einwilligung funktionieren können. Dass das Buch im Hinblick auf Dienste zur Einwilligungsverwaltung, also Personal Information Management Systems (PIMS), nicht über einen Ausblick hinauskommt, ist dem Veröffentlichungszeitpunkt geschuldet, denn entsprechende Anbieter sind bisher weder etabliert noch zertifiziert.

Zu früh erschienen ist dieser erste große allein stehende Kommentar zum TTDSG deshalb jedoch keinesfalls. Es liegt hier doch deutlich mehr vor als lediglich eine Notlösung, auf die aus Mangel an Alternativen zurückgegriffen wird. Vielmehr handelt es sich um einen Kommentar, der nicht nur umfassend den aktuellen Sachstand beschreibt, sondern sicher auch durch die Gerichte für die noch zu konkretisierende Rechtsprechung zum TTDSG herangezogen werden wird. Entsprechend ist der Eingang ins Bücherregal von Datenschutz-Interessierten und Praktikern sicher kein Fehler.

Rezension von

Markus Steinkamp
ist Konzerndatenschutzbeauftragter bei Hellmann Worldwide Logistics in Osnabrück.
Der studierte Wirtschaftswissenschaftler erlangte einen Master in angewandter IT-Sicherheit an der Ruhr-Universität und arbeitet seit mehr als zehn Jahren in den Bereichen Datenschutz und Informationssicherheit. Markus Steinkamp ist zertifizierter Datenschutzbeauftragter (TÜV) und nach Verbandskriterien des BvD verpflichtet.

FORMULARHANDBUCH DATENSCHUTZRECHT

Dr. Ansgar Koreng, Dr. Matthias Lachenmann (Hrsg.)

Auch in der dritten Auflage findet man in dem Autorenteam zahlreiche Vertreterinnen und Vertreter aus Aufsichtsbehörden und der Praxis, die hier nicht nur Mustertexte bereitstellen, sondern auch die rechtlichen Hintergründe dazu und diese so detail- und kenntnisreich erläutern, dass das Formularhandbuch auch als Kommentarergänzung herangezogen werden könnte.

Laut Vorwort wenden sich die Herausgeber an Rechtsanwender und diese finden tatsächlich in dem Formularhandbuch Datenschutzrecht zu allen denkbaren Fragestellungen Hilfen und Erläuterungen. Geordnet ist das Formularhandbuch nach Themengebieten, angefangen bei der Organisationstruktur im Datenschutz und dem Datenschutzbeauftragten. Hier finden sich dann Beispiele zur Organisationsstruktur, aber bereits auch schon zu Selbstverpflichtungen in Code of Conducts und Hinweisgebersystemen. Ausführlich werden die Dokumentationspflichten behandelt, die dem Verantwortlichen und dem Auftragsverarbeiter helfen ihrer Nachweispflicht nachzukommen, bei dem aber auch das in der Praxis oft vernachlässigte Thema der freien Mitarbeiter dargestellt wird. Bei den technischen und organisatorischen Maßnahmen finden sich zudem Checklisten, aber erfreulicherweise auch Hinweise zur Dokumentenlenkung.

Die Regelungen zur Umsetzung der ePrivacy-Richtlinie werden bereits über das TTDSG auf Basis des TTDSG-E vom Februar 2021 behandelt. Die Musterformulierungen zur Web Analysis berücksichtigen dabei die gängigen Anbieter. Bei der Darstellung der Auftragsverarbeitung wird zunächst über eine Gegenüberstellung der Anforderungen zur gemeinsamen Verantwortlichkeit eine Unterstützung zur Abgrenzung und Einordnung gegeben, bevor diese beiden Formen der Zusammenarbeit getrennt voneinander ausführlich dargestellt werden. Beim Beschäftigtendatenschutz werden die gängigsten Themen aus der Praxis wie Einwilligungserklärung von Beschäftigten zur Verwendung von Fotoaufnahmen, Fragen im Rahmen von Arbeitsunfähigkeit und betrieblichem Wiedereingliederungsmanagement oder auch Screening

Dr. Ansgar Koreng, Dr. Matthias Lachenmann (Hrsg.)
Formularhandbuch Datenschutzrecht

VERLAG C.H.BECK

3. Auflage 2021
1.602 Seiten
inkl. Freischaltcode zum Online-Zugang (für einen Nutzer)
Preis: 139,00 Euro
ISBN: 978-3-406-74904-9

von Beschäftigten erläutert und mit entsprechenden Mustertexten für die Umsetzung in der Praxis unterstützt. Beim Kundendatenschutz wird die Problematik des B2B-Bereichs angesprochen und mit Lösungshinweisen versehen. Neben denn „allgemeinen" Themen widmet sich das Formularhandbuch Datenschutzrecht auch branchentypischen Themenstellungen wie der datenschutzrechtlichen Einwilligung im Gesundheitsbereich, im Bereich der klinischen und nicht-klinischen Forschung, Datenschutz im Verein und erfreulicherweise auch Datenschutz in der Anwaltskanzlei. Natürlich fehlen in diesem Werk auch nicht die Darstellung der möglichen Themenstellungen und entsprechenden Mustertexte in der Kommunikation mit Datenschutzaufsichtsbehörden im Kapitel über behördliches und verwaltungsgerichtliches Verfahren.

Ein eigenes Kapitel ergänzt die Betrachtung im Hinblick auf Besonderheiten der Rechtsumsetzung in Österreich, was dem Werk einen breiteren Einsatzbereich und dem Rechtsanwender einen weiteren Nutzen ermöglicht.

Natürlich sind alle Mustertexte aus dem Formularhandbuch Datenschutzrecht in jedem Einzelfall dahingehend zu prüfen und gegebenenfalls auf die konkrete Situation hin anzupassen. Je nach Vorkenntnissen des Rechtsanwenders könnten hier im Einzelfall Diskussionen erforderlich werden, aber das liegt mehr an den vielen noch nicht vom EuGH abschließend entschiedenen Einzelfragen als an dem Werk selbst.

Ich halte es für absolut empfehlenswert, da es meines Erachtens nach den Rechtsanwendern jeder Niveaustufe einen Mehrwert bietet, alle relevanten Fragestellungen im Wesentlichen zum Zeitpunkt des Redaktionsschlusses Mai 2021 behandelt werden und über den Onlinezugang alle Mustertexte und Checklisten auch als Dateiformat zugänglich sind.

DATENSCHUTZRECHT

EIN KOMMENTAR FÜR STUDIUM UND PRAXIS

Annika Selzer (Hrsg.)

Ehrlich gesagt, war ich etwas überrascht, hatte ich bislang nichts gefunden, was man Studierenden zum Thema Datenschutz an die Hand geben kann, die nicht bereits über einen juristischen Hintergrund verfügen und sich trotzdem vertiefend mit datenschutzrechtlichen Fragestellungen befassen wollen oder müssen. Nun bin ich fündig geworden. Bei „Datenschutzrecht – Ein Kommetar für Studium und Praxis" handelt es sich um ein rund 600 Seiten starkes Werk, das mit doppelseitiger Abbildung im Querformat noch lesbar bleibt und mittels einer Spiralbindung in den Produktionskosten einen auch für Studierende annehmbaren Preis ermöglicht.

Die Autoren, die sich hinter der Herausgeberin und dem Fraunhofer Institut zusammenfanden, sind „in der Szene" teilweise gut bekannt, etwa weil sie als Beschäftigte von Datenschutzaufsichtsbehörden oder als Fachreferenten bei Veranstaltungen aufgetreten sind oder über anderweitige Veröffentlichungen Bekanntheit erlangten. Andere kommen aus der Praxis, bringen oft einen wissenschaftlichen Hintergrund im Lebenslauf mit und sind an Hochschulen zum Datenschutzrecht oder zu IT-Sicherheitsthemen aktiv.

Die Autorenliste umfasst (in alphabetischer Reihenfolge) Daniel Bartholmai, Stephan Blazy, Sarah Diel, Erdem Durmus, Jens Engelhardt, Merle Freye, Wendy Heereman, Claudia Heudecker, Oliver Hinte, Leif-Erik Holtz, Samira Kahlenbach, Dennis-Kenji Kipker, Jörg M. Leuchtner, Kevin Marschall, Philipp Niggl, Maria Christina Rost, Maximilian Schnebbe, Dario Scholz, Linda Schreiber und Annika Selzer. Der Umfang der kommentierten Regelungen enthält die Datenschutzgrundverordnung (DS-GVO) und den 1. und 2. Teil des Bundesdatenschutzgesetzes (BDSG). Der 3. Teil, der die Umsetzung der Vorgaben der RL 2016/680 –„Polizei und Justiz" beinhaltet, bleibt nachvollziehbar außen vor. Auch werden die aus Sicht der Autoren relevanten Paragrafen aus dem Betriebsverfassungsgesetz, dem Kunsturheberrecht und dem Gesetz gegen den unlauteren Wettbewerb abgebildet und kommentiert. Damit wird bereits ein Großteil der rechtlichen Grundlagen, die sich in alltäglichen Fragestellungen, aber auch in der Ausbildung wiederfinden, in den Grundzügen bearbeitet werden können. Dies umfasst auch die Thematik der Werbung (inkl. des neuen § 7a UWG), der Nutzung von Abbildungen und der Mitbestimmungsrechte des Betriebsrates. Es darf aber nicht hinwegtäuschen, dass der Umfang nicht geeignet ist vertieft alle Fragen abzubilden geschweige denn zu allen Fragestellungen Lösungsmöglichkeiten zu diskutieren. Vermisst hatte ich beispielsweise bei Art. 28 DS-GVO den Hinweis auf die Leitlinie 07/2020 (zu den Begriffen „Verantwortlicher" und „Auftragsverarbeiter" in der DSGVO) des Europäischen Datenschutzausschusses, die zu etlichen wichtigen Auslegungsfragen Orientierung und Diskussionsgrundlage bietet, so auch zu der Frage der weiteren Auftragsverarbeiter. Aber hier bietet sich dann ja an, dass durch die Lehrenden an den Hochschulen diese Themen ergänzt und vertieft werden können.

Der Kommentar als Nachschlagewerk ist für das Studium und Ausbildung aufgrund seiner praxisnahen Zusammenstellung sehr empfehlenswert. Es ist zu hoffen, dass er gelegentlich den entsprechenden rechtlichen Entwicklungen angepasst wird, um auch zukünftig den Anforderungen gerecht zu werden.

Annika Selzer (Hrsg.)
Datenschutzrecht – Ein Kommentar für Studium und Praxis

FRAUNHOFER VERLAG

1. Auflage 2022
601 Seiten
49,00 Euro
ISBN-13: 978-3-8396-1759-5

Rezensionen von

Rudi Kramer
ist Rechtsanwalt und Sprecher des AK Schule im BvD. e.V.

PRAXISHANDBUCH KÜNSTLICHE INTELLIGENZ

Lothar Schröder, Petra Höfers

Wer die Wahrheit hat, hat die Qual. Mit ihrem Praxishandbuch Künstliche Intelligenz bringen Lothar Schröder (Mitglied der Enquete-Kommissionen „Künstliche Intelligenz“, bis 2019 war er im ver.di Bundesvorstand verantwortlich für die IT- und TK-Branche) und Petra Höfers (Juristin mit arbeitsrechtlichem Schwerpunkt, Mitbestimmungsexpertin) ein weiteres, in Gestaltungstruktur ansprechendes Werk zur eingehenden Befassung mit dem Thema Künstliche Intelligenz (KI) heraus.

Erschienen ist das Praxishandbuch im Bund Verlag, der insbesondere für seine arbeitsrechtlichen und sozialrechtlichen Publikationen bekannt ist und bei Interessenvertretungen von Arbeitnehmer/innen, Betriebsräten und Personalräten großes Ansehen genießt. Dementsprechend verwundert es nicht, dass dem Thema der betrieblichen Mitbestimmung im Zusammenhang mit der Einführung und Gestaltung von KI erhebliche Aufmerksamkeit in dem Praxishandbuch geschenkt wird.

Einige Kapitel wurden teilweise von Gastautoren geschrieben, zu denen unter anderem der ehemalige Vorsitzende des DGB, Rainer Hoffmann, und der ehemalige ver.di-Vorsitzende Frank Bsirske zählen. Vor diesem Hintergrund richtet sich das Praxishandbuch - wenn auch nicht ausschließlich – im Schwerpunkt an Akteure der betrieblichen Mitbestimmung, was es für andere Gruppen wie Datenschutzbeauftragte und-berater nicht minder lesenswert macht.

Entsprechend der einleitenden Darstellung handelt es sich um ein Werk mit mehr als 450 anspruchsvollen Seiten, auf denen ein Überblick zur KI gegeben werden soll. Es soll als Praxishilfe dienen, die Gestaltungarbeit erleichtern und der Leserschaft ersparen, sich mühsam durch eine Vielzahl von Quellen selbst durchzuarbeiten. Dabei bietet es zahlreiche Checklisten und Prüffragen zur Überprüfung von KI-Systemen, die auch Datenschutzbeauftragten und -beratern nützlich sein können.

Lothar Schröder, Petra Höfers
Praxishandbuch künstliche Intelligenz

BUND VERLAG

1. Auflage 2022
452 Seiten
48 Euro
ISBN 978-3-7663-7264-2

Hervorzuheben ist das sehr verständlich geschriebene Kapitel zur Einordnung der Bedeutung und den unterschiedlichen in der Praxis vorkommenden Ausformungen von KI. Die Autoren nutzen dazu wie auch an zahlreichen anderen Stellen Analogien und Praxisbeispiele, um komplexe Sachverhalte für Laien verständlich und anschaulich zu machen, die wissenschaftliche, zu detaillierte Ausführungen bei der anfänglichen Durchdringung des Themas überfordern können.

Im Übrigen ist erwähnenswert, dass sich die Autoren mit den Auswirkungen von KI auf die Arbeitswelt (Kap. 6) befassen, wobei sie sowohl potenzielle Ängste und Sorgen sowie den möglichen Kontrollverlust durch KI thematisieren. Der datenschutzrechtlichen Bewertung von KI wird in Kap. 14 in komprimierter Form Aufmerksamkeit geschenkt, wobei das Thema gleichsam im Lichte der Grundrechte (Kap. 12) beleuchtet wird. Dazu passt wiederum auch der Fokus der Autoren auf Gesichtspunkte der Ethik (Kap. 11, 22).

Im Ergebnis ist das Praxishandbuch eine Leseempfehlung.

Rezension von

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

BvD-Webinare & Online-Seminare

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Termin	Thema
27. – 28.07.2022	**Präsenz-Seminar & Workshop** **– IT für Datenschutzbeauftragte** Düsseldorf
13. – 15.09.2022	**Präsenz-Seminar** **– Get Ready: Datenschutz für Koordinatoren**
20.09.2022	**Präsenz-Seminar** **– Datenschutz im Internet –** **Was DSBs wissen sollten!** Frankfurt/Main
26. – 27.10.2022	**BvD-Herbstkonferenz 2022** Stuttgart
28.10.2022	**BvD-Behördentag 2022** Stuttgart

PREISE:

Webinare	95,00 - 145,00 €*	BvD-Mitglieder
	145,00 - 195,00 €*	Nichtmitglieder
Online-Seminare	295,00 - 495,00 €*	BvD-Mitglieder
	395,00 - 595,00 €*	Nichtmitglieder

(*Alle Preise zzgl. gesetz. MwSt.)

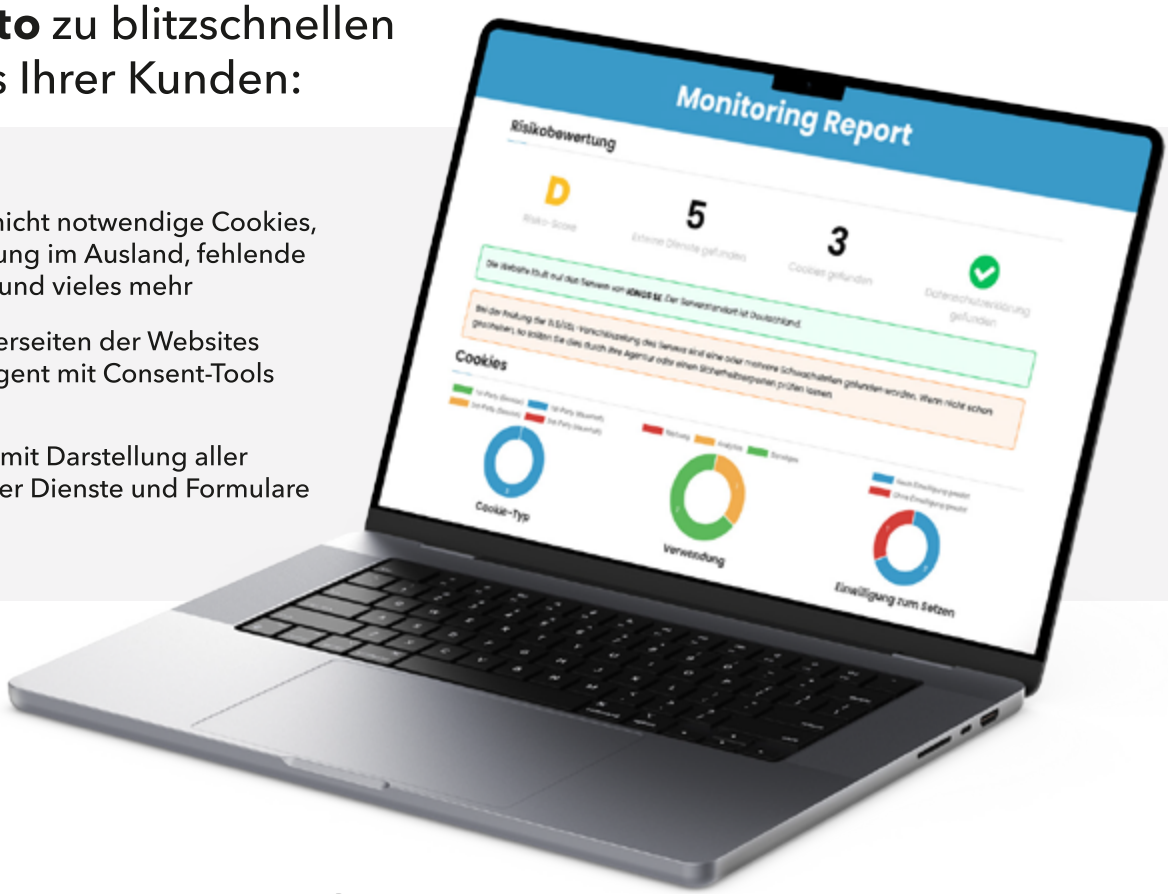
JETZT ANMELDEN:
www.bvdnet.de/termine

Anzeige

Websites manuell auf Datenschutzlücken zu durchsuchen ist Vergangenheit!

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

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



Sind Sie bereit dafür, Ihre Zeit besser zu nutzen?

- Mit dem **Report in Ihrem eigenen Branding** können Sie Ihrer Prüfpflicht nachkommen und Ihren Kunden fachliche Kompetenz demonstrieren.
- Unser DSGVO-Scanner erledigt für Sie 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 **0177 3415205**
oder besuchen Sie unsere Website für eine **kostenfreie 14-Tage-Testphase**.