Ausgabe 01/2022

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

MALWARE, PHISHING, VIRUS: DATENSCHUTZ BRAUCHT DATENSICHERHEIT

HACKER IM NETZ! WAS JETZT TUN? – S. 5

DATENSICHERHEIT – DILETTIEREN ODER DELEGIEREN? – S. 10

„DATENSCHUTZ IST EIN SEISMOGRAPH DER RECHTSTAATLICHKEIT“ – INTERWIEV MIT JULIANE HUNDERT – S. 36

„UUUND ACTION“ FÜR „DATENSCHUTZ GEHT ZUR SCHULE“ – S. 48

BvD e.V.
DATENSCHUTZ GESTALTEN

BvD e.V.
DATENSCHUTZ GESTALTEN

2022

BvD-Verbandstage

10.05. - 11.05.2022

IM DORINT KURFÜRSTENDAMM
HOTEL BERLIN

Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

NAMHAFTE REFERENT:INNEN MIT VORTRÄGEN ZU DIESEN FOKUS-THEMEN:

- Digitale Mobilität (Auto, Mobile Device & Co, Einwilligung)
- Ist Datensouveränität des Individuums möglich?
- Datenschutz in Zeiten von Cybercrime
- Regierungswechsel & Datenschutz – Wo geht die Reise hin?

JETZT ANMELDEN:

www.bvdnet.de/bvd-verbandstag

TEILNAHMEGEBÜHREN:

BvD-Verbandstage 10./11.05.2022

BvD-Mitglieder: 850 € | Nichtmitglieder: 1.050 €

Alle Preise zzgl. gesetz. MwSt.

EDITORIAL

Liebe Leserinnen und Leser,

„In Zeiten wie diesen haben wir andere Probleme als den Datenschutz." So oder so ähnlich hört man es derzeit von vielen Seiten – selbst aus den Reihen der Datenschützer. Das ist auch vollkommen richtig, dass im Angesicht eines Krieges in der Ukraine und der humanitären Notlage, in die er die Menschen dort bringt, andere Themen verblassen. Alles andere wäre schlicht unmenschlich.

Und doch möchte ich versuchen, Sie einzuladen und den Blick etwas zu weiten und vielleicht doch eine Verbindung herzustellen, zwischen dem, was uns in dieser Ausgabe der BvD-News beschäftigt. Unser Titelthema beleuchtet diesmal die Verbindung von Datenschutz und Datensicherheit. Und gerade Letztere spielt in diesen Zeiten eine entscheidende Rolle. Denn Kriege werden heutzutage nicht mehr allein mit Panzern und Raketen ausgetragen. Krieg ist heute immer auch ein Cyber-Krieg – nur nicht ganz so offensichtlich und deswegen nicht weniger gefährlich.

Unternehmen und öffentliche Stellen, die den Datenschutz ernst nehmen, haben immer auch ein Bewusstsein für die große Bedeutung von Datensicherheit. Denn es gilt: kein Datenschutz ohne Datensicherheit. Und das ist in Zeiten von Cyberangriffen durch Kriminelle, aber eben auch durch Staaten ein Thema, das mehr und mehr an Bedeutung gewinnt.

Wir beleuchten unseren Themenschwerpunkt in drei Beiträgen aus verschiedenen Perspektiven: Der Text von Robin Brocks, Dr. Hauke Hansen und Suntka von Halenerste beschäftigt sich mit dem »Fall der Fälle«, dass Hacker ins System eindringen. Niels Lepperhoff wiederum warnt, TOM allein können keine Datensicherheit garantieren und Eberhard von Faber zeigt auf, wo bei der Nutzung von Cloud-Diensten Sicherheitslücken auftreten können.

Noch mehr zum Thema gibt es dann bei den BvD-Verbandstagen am 9. und 10. Mai in Berlin, die diesmal unter dem Motto „Datenschutz und Datensicherheit – Digitale Zukunft begleiten" stehen. Es erwarten Sie wieder anregende Begegnungen, eine festliche Abendveranstaltung mit Verleihung unseres Datenschutz Medienpreises DAME und natürlich viele hochkarätige Redner. Unter anderem hat uns nach Druckschluss unseres Programmflyers, der dieser BvD-News beiliegt, noch die Zusage von Max Schrems erreicht – eine Premiere beim BvD, auf die ich persönlich ganz besonders gespannt bin. Ich würde mich freuen, Sie im Dorint Kurfürstendamm Berlin begrüßen zu dürfen.

Doch nun wünsche ich Ihnen erst einmal eine anregende Lektüre.

Thomas Spaeing
BvD-Vorstandsvorsitzender

EDITORIAL

Thomas Spaeing 3

DATENSCHUTZ UND DATENSICHERHEIT

Hacker im Netz! Was jetzt tun? – *Robin Brocks, Dr. Hauke Hansen, Suntka von Halen* 5

Datensicherheit – Dilettieren oder Delegieren? – *Dr. Niels Lepperhoff* 10

Warum sich Datenschützer mit Details beim Cloud-Computing auseinandersetzen müssen – *Eberhard von Faber* 14

DSGVO

Datenschutzbeauftragte und Aufsichtsbehörden: Chancen und Grenzen der Zusammenarbeit – *Andrea Backer-Heuveldop, Dr. Bernd Schütze* 20

GESETZ UND RECHTSPRECHUNG

Wird der Datenschutz zukünftig durch Private durchgesetzt? – *Stefan Sander, LL.M., B.Sc.* 24

DATENSCHUTZPRAXIS

Zertifizierung bringt Mehrwert – *Bettina Gayk, Henrike Postberg* 32

AUFSICHTSBEHÖRDEN

„Datenschutz ist ein Seismograph der Rechtstaatlichkeit" – *Interwiev mit Juliane Hundert* 36

Werden Datenschutzverstösse immer teurer? – *Maria Christina Rost* 38

GESELLSCHAFT

Anwendungsszenarien und Bedenken beim Einsatz künstlicher Intelligenz in der öffentlichen Verwaltung – *Wendy Heereman und Giusi Abagnale* 44

AUS DEM VERBAND

„Uuund Action" für Datenschutz geht zur Schule – *Rudi Kramer* 48

Datenschutz ist gelungene Kommunikation – *Dr. Vera Losse* 52

DATENSCHUTZ KURZ GEFASST

Datenschutz-Motive für „Datenschutz geht zur Schule" gesucht – *David Heimburger* 56

Neue Serviceangebote für BvD-Mitglieder – *Dipl.-Ök. Stephan Rehfeld* 57

REZENSIONEN

Meine Aufgaben als Datenschutzbeauftragter – *Rudi Kramer* 58

TTDSG leicht erklärt – *Jens Eckhardt* 60

Datenschutz im Unternehmen – *Michael Wächter* 62

Künstliche Intelligenz – *Dr. Kuuya Josef Chibanguza, Christian Kuß, Hans Steege (Hrsg.)* 64

TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 66

Wichtige Kontakte 67

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.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):

www.123rf.com

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

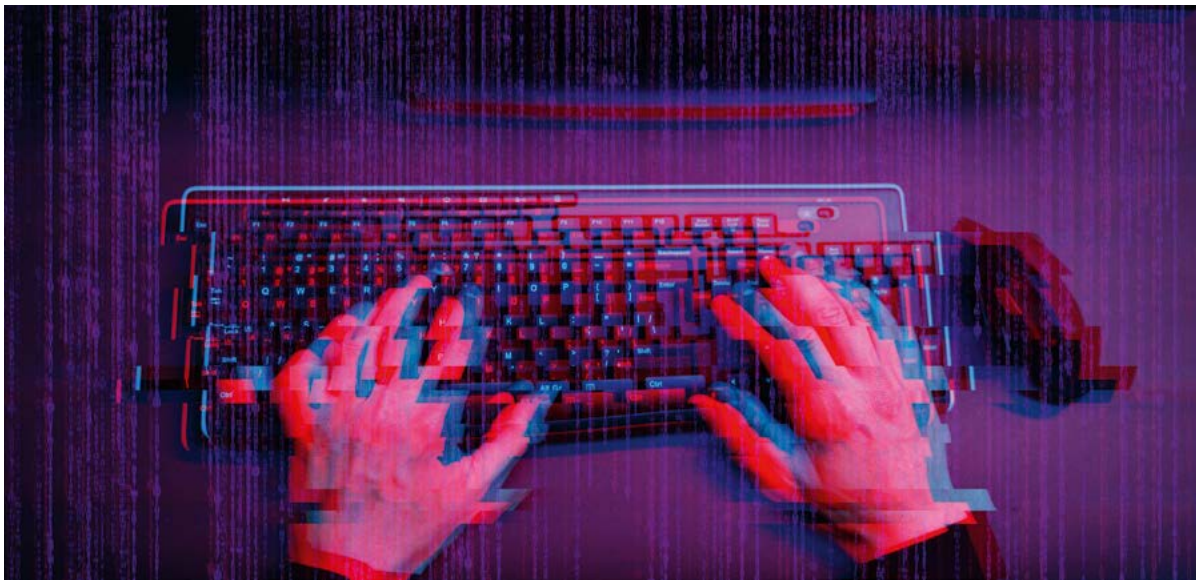
ISSN: 2194-1025

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.

HACKER IM NETZ! WAS JETZT TUN?

Übersicht mit Handlungsempfehlung für den Fall der Fälle aus drei Blickwinkeln

Robin Brocks, Dr. Hauke Hansen, Suntka von Halen



Zu den größten Risiken, denen Unternehmen und Organisationen derzeit ausgesetzt sind, gehören Cyberattacken, die auf Daten und die Verfügbarkeit von IT-Systemen abzielen. Bereits 2019 erwarteten Experten, dass für das Jahr 2021 die Schäden durch Ransomware allein weltweit bei rund 20 Milliarden Euro liegen würden, wobei hier immer noch ein großes Dunkelfeld existiert.[1] Die wirtschaftlichen Einbußen durch gestohlene personenbezogene und sonstige vertrauliche Daten sowie der Diebstahl von geistigem Eigentum sind schwer oder auch gar nicht bezifferbar.

Wenn ein Cyberangriff ein Unternehmen trifft, muss alles sehr schnell gehen. Cybervorfälle verursachen schnell geschäftskritische Auswirkungen, daher ist das damit verbundene Krisenmanagement eine gesamtunternehmerische Aufgabe. Die Erfahrung zeigt, dass zu häufig die Verantwortung der internen IT überlassen wird. Dabei sind Verfügbarkeit und Führung durch das Managementteam, einschließlich des CEOs, unabdingbar.

Incident Response

Sollte der begründete Verdacht bestehen, dass unberechtigte Dritte IT-Systeme einer Organisation übernommen haben, ist ein ruhiges und überlegtes Vorgehen für den Erfolg der Aufklärung von oberster Priorität. In diesem Fall gilt nichts zu überstürzen. Um den Kreis der Eingeweihten klein zu halten, sollten nur wenige Personen von dem Verdacht erfahren. Im nächsten Schritt sollte schnellstmöglich professionelle Hilfe hinzugezogen werden.

Denn nicht jedes Unternehmen hat ein eigenes *Incident-Response-Team*. Der aus dem Englischen übernommene Begriff bezeichnet die „digitale Feuerwehr", die bei einem Vorfall ausrücken muss. Unterstützen können hier Dienstleister, die in

[1] Vgl. Cybercrime Magazine, unter https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

der Regel über das notwendige Personal, Wissen und Equipment inklusive professioneller Software für die gängigen Betriebssysteme wie Windows, Unix und MacOS verfügen, um beispielsweise eine digitale forensische Untersuchung durchzuführen.

Die Auswahl eines solchen Dienstleisters richtet sich nach der Art des Vorfalls und den Zeitzonen, in denen an dem Fall gearbeitet werden soll. Ein kleiner, regionaler Anbieter besitzt beispielsweise eher nicht die notwendigen Fähigkeiten, um international tätige Unternehmen auf mehreren Kontinenten nach dem „*follow-the-sun*"-Prinzip unterstützen zu können. Die gleichzeitige Untersuchung von mehreren hunderttausenden Servern und Laptops ist global nur einer Handvoll von spezialisierten Incident-Response-Dienstleistern möglich.

Zu den ersten Schritten einer erfolgreichen Incident Response gehört **Sichtbarkeit**. Erst wenn klar ist, welche IT-Systeme überhaupt kompromittiert sind, kann die darauffolgende **Eindämmung** erfolgreich sein. An dieser Stelle kommt zumeist EDR Software (Endpoint Detection and Response) zum Einsatz, um automatisiert jede Art von Schadsoftware zu stoppen.

Die Erfahrung zeigt, dass Unternehmen oftmals keine vollständige Inventarisierung vorhandener IT-Systeme in ihren Netzwerken haben, was nicht nur im Ernstfall besonders nachteilig ist. Denn gerade „vergessene", aber noch eingeschaltete Systeme von längst eingestellten Projekten werden oft zum Einfallstor für Cyberangriffe, da diese auch nicht mehr aktualisiert und abgesichert werden.

Sodann empfiehlt es sich in den Unternehmen bereits vorhandene Ereignisprotokolle, die Details der Kompromittierung aufgezeichnet haben, auszuwerten. Aufzeichnungen von Firewalls, Betriebssystemen oder einem SIEM (Security Incident and Event Monitoring) enthalten häufig wichtige Hinweise auf die Art des Cyberangriffs.

Erst wenn Sichtbarkeit vorhanden und der laufende Cyberangriff gestoppt ist, beginnen *Incident-Response-Teams* mit der Suche nach den Gründen für die erfolgreiche Kompromittierung („Root Cause Analysis"). Ursächlich für erfolgreiche Cyberangriffe sind zumeist:

- Nicht aktualisierte Systeme, die mit dem Internet verbunden sind. Sobald eine neue Sicherheitslücke publik wird, beginnen professionelle Akteure mit der Suche nach verwundbaren Systemen, um darüber in Unternehmensnetze einzubrechen.
- Professionelle manipulierte E-Mails („Whale Phishing"), die von vorhandenen Sicherheitsprodukten nicht erkannt werden. Im Fokus stehen dabei oft Vorstände und Führungskräfte mit beruflichem Bezug zu Unternehmensfinanzen und Produktentwicklung.
- Nutzung von manipulierter Software, wobei der Hersteller der Software zuvor erfolgreich angegriffen wurde und nun die manipulierte Software samt ihrer digitalen Hintertüren an zahlreiche Kunden ausliefert. Dies ist eine sogenannte „Supply Chain Attack", die über die Lieferbeziehung zu Hunderten gleichzeitig betroffener Kunden führen kann. Anfang 2021 war dies beim Unternehmen Solarwinds der Fall und zahlreiche deutscher Organisationen waren durch die Nutzung der Software von Solarwinds zum Opfer von Ausspähung geworden.

In den meisten Fällen kann die Ursache für den Cyberangriff festgestellt werden. Fehlende Ereignisprotokolle, von den Angreifern gelöschte oder auch versehentlich vom Unternehmen selbst überschriebene Daten machen mitunter jedoch eine genaue Ursachenbestimmung unmöglich.

Am Ende der Untersuchung steht die Anfertigung eines schriftlichen Berichts des *Incident-Response-Dienstleisters*. Dieser enthält üblicherweise die Ergebnisse der Investigation, eine Zeitachse der Ereignisse und Empfehlungen an das Unternehmen, wie ein solcher Cyberangriff in Zukunft verhindert werden kann. Die empfohlenen Maßnahmen können sowohl technischer, organisatorischer als auch prozessualer Natur sein.

Rechtliche Meldepflicht

Neben der *Incident-Response* sind im Fall eines Angriffs auf die IT-Infrastruktur diverse rechtliche Fallstricke zu beachten.

Wenn – wie das bei Ransomware-Angriffen mittlerweile üblich ist – nicht nur die IT-Systeme verschlüsselt, sondern zuvor auch umfangreich Unternehmensdaten abgezogen wurden, darf der Datenschutz nicht außer Acht gelassen werden. Ein solches Datenleck – oder im Jargon der Datenschutz-Grundverordnung (DSGVO) „eine Verletzung des Schutzes personenbezogener Daten" – führt zum einen zu einer Meldepflicht bei der Datenschutzbehörde. Zum anderen müssen unter bestimmten Umständen sämtliche betroffenen Personen informiert werden, deren Daten in die Hände der Hacker gelangt sind. In der Regel handelt es sich dabei um Mitarbeiter, Kunden und Lieferanten.

Die Meldepflicht gilt ausnahmsweise nicht, wenn nur geringe Risiken für die Betroffenen bestehen, deren Daten abhandengekommen sind. Die demnach notwendige Gefahrenprognose muss das Unternehmen selbst treffen, und das sehr schnell: Denn zwischen Bekanntwerden des Vorfalls und der Meldung gegenüber der zuständigen Datenschutzbehörde dürfen maximal 72 Stunden liegen. Dabei befinden sich Verantwortliche in einer Zwickmühle. Denn einerseits kann die unterlassene Meldung mit hohen Bußgeldern von bis zu vier Prozent des Jahresumsatzes oder 20 Millionen Euro sanktioniert werden, wenn der Fall später doch der Behörde zur Kenntnis gelangt. Andererseits kann ein vorschnelles Melden von Datenpannen gefährlich sein. Da die Datenschutzbehörden im Anschluss an eine Meldung regelmäßig mehr oder weniger umfangreiche Auskünfte über die IT-Sicherheit im Unternehmen verlangen, laufen Verantwortliche Gefahr sich durch eine Meldung selbst „ans Messer zu liefern".

Zwar sieht das Bundesdatenschutzgesetz vor, dass Selbstanzeigen wegen Datenschutzvorfällen von den Behörden nicht für Bußgeldverfahren verwertet werden dürfen. Das wird von manchen Datenschutzbehörden aber ignoriert: So verhängte der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg bereits Bußgelder, die sich auf den Inhalt einer solchen Meldung stützten. Er hält die Regelung im Bundesdatenschutzgesetz für europarechtswidrig und sieht sich daran nicht gebunden.

Durchaus überraschend: Mängel bei der Datensicherheit bilden einen der häufigsten Gründe, aus denen Datenschutzbehörden Bußgelder aussprechen. Die Opfer werden also zur Kasse gebeten. Zwei der höchsten Bußgelder, die unter der DSGVO überhaupt verhängt wurden, betrafen gehackte Unternehmen. (Hotelkette Marriott, 110 Millionen Euro, Fluglinie British Airways 200 Millionen Euro, beide Bußgelder später stark reduziert). Insofern sind Unternehmen gut beraten bei einem Cyberangriff kritisch zu prüfen, ob tatsächlich eine Meldepflicht besteht.

Cyberversicherung

Auch die Inhaber einer Cyberversicherung sollten sich nicht vorschnell in Sicherheit wähnen. Solche Policen – noch vor wenigen Jahren von den Versicherern als mehr oder weniger aufwandsneutrale „Dreingabe" für ein vermeintlich theoretisches Risiko betrachtet – entpuppen sich für die Anbieter zunehmend als Kostenfalle. Dementsprechend ist mitunter die Neigung hoch den Versicherungsschutz abzulehnen. Hier lohnt ein genauer Blick in die Vertragsbedingungen, denn die Regelungen unterscheiden sich je nach Anbieter erheblich. So lassen sich IT-Sicherheitsvorfälle häufig auf menschliches Versagen zurückführen. Versicherern, bei denen der Einwand grober Fahrlässigkeit nicht ausgeschlossen ist, steht damit je nach Fallgestaltung ein relativ einfaches Vehikel zur Verfügung Zahlungen abzulehnen. Auch lassen sich Versicherungen vor Abschluss des Vertrages von den Unternehmen zusichern, dass bei ihnen ein umfassendes Informationssicherheitsmanagementsystem (ISMS) besteht. Zudem setzt der Deckungsschutz häufig den Einsatz ganz bestimmter, vom Versicherer benannter IT-Spezialunternehmen voraus. Diese können sich zwar unter Umständen tatsächlich als kompetente und hilfreiche Dienstleister erweisen. Gleichzeitig erhalten diese von der Versicherung mandatierten Dienstleister aber umfassenden Einblick in die IT-Infrastruktur des Unternehmens - und damit auch in etwaig bestehende Sicherheitsdefizite. Finden diese Schwächen Eingang in den forensischen Bericht, den solche Unternehmen in der Regel anfertigen, steht dem Versicherer mitunter eine wahre Fundgrube an Gründen zur Verfügung den Versicherungsschutz wegen grober Fahrlässigkeit abzulehnen.

Unternehmen, die keine dedizierte Cyberversicherung besitzen, sollten ihre konventionelle Sach- oder Haftpflichtpolice prüfen. Mitunter sind hierdurch Cyberschäden abgedeckt, denn viele Versicherungsbedingungen wurden entworfen, als mit derartigen Schäden noch nicht zu rechnen war und diese von den Versicherungen nicht ausgeschlossen wurden. Man spricht hier von Silent-Cyber-Risiken.

Lösegeldzahlung und Geldwäsche

Zwar streben die meisten Unternehmen an, ihre Systeme und Daten ohne die kostenpflichtige „Hilfe" des Angreifers, also ohne Zahlung des verlangten Lösegeldes, wiederherzustellen. Dies gelingt umso besser, je stärker die Backups und ihre Speicherintervalle geschützt sind. Auch die zentralen Anlaufstellen der Staatsanwaltschaften für Cybercrime raten von solchen Zahlungen ab, und es gibt natürlich auch keine Garantie dafür nach der Zahlung den „rettenden" Schlüssel zu erhalten.

Gleichwohl wurden im vergangenen Jahr mehrere Hundert Millionen Euro an Lösegeldern bezahlt. Das geschah oftmals auch zur Zufriedenheit des erpressten Unternehmens, da viele Hacker an einem „vertrauenswürdigen" Image interessiert sind und nach einer

Lösegeldzahlung tatsächlich die Schlüssel zur Entschlüsselung der Unternehmensdaten übermitteln und keine Nachforderungen stellen. Mit einer solchen Zahlung begeben sich Unternehmen aber rechtlich auf „dünnes Eis". Denn mit einer solchen Zahlung werden die kriminellen Aktivitäten der Tätergruppe gefördert und begünstigt. Unter Umständen kann hierin auch eine illegale Geldwäsche liegen. Die Lösegeldzahlung an Tätergruppen aus Embargoländern kann zudem einen Verstoß gegen außenwirtschaftsrechtliche Vorschriften bedeuten. Schließlich sollten Unternehmen mit US-Niederlassungen ganz besonders vorsichtig sein. Hier bestehen Bestrebungen die Zahlung von Lösegeldern gänzlich zu verbieten.

Geschäftsgeheimisse

Darüber hinaus drohen Rechtsfolgen auf weiteren Feldern: Nicht selten gehen Unternehmen strenge Pflichten ein Geschäftsgeheimnisse – zum Beispiel von Geschäftspartnern – gegen unbefugten Zugriff zu schützen. Mitunter verpflichten sich Unternehmen im Rahmen von Non-Disclosure-Agreements sogar dazu den Bruch eines solchen Geheimnisses an den Partner aktiv zu melden. Bei Verletzung drohen Vertragsstrafen.

Umgekehrt droht auch der rechtliche Schutz eigener Geschäftsgeheimnisse verloren zu gehen, denn das Geschäftsgeheimnisgesetz schützt nur solche Geheimnisse, die angemessen gegen unbefugten Zugriff gesichert sind. Bei einem Cyberangriff könnte sich also herausstellen, dass keine angemessenen Schutzmaßnahmen bestanden. Dann könnte das Unternehmen nicht einmal gegen einen Konkurrenten vorgehen, der sich das Geheimnis – etwa ein geheimes Produktionsverfahren – aus dem Darknet verschafft hat, wo Erpresserbanden ihre digitale Beute gern veröffentlichen, um Druck auf das bestohlene Unternehmen auszuüben.

Kommunikation im Krisenmanagement

Strategisches Ziel der Kommunikation im Krisenmanagement ist der langfristige Reputationsschutz. Aufgabe des Teams ist für konsistente Informationen und kontinuierliche Updates an interne und externe Zielgruppen zu sorgen und Sprechfähigkeit sowie die Kommunikationshoheit des Unternehmens sicherzustellen.

Zu Beginn der Response-Phase liegt die Priorität auf Schnelligkeit: Ein erstes kurzes Holding Statement muss den aktuell verfügbaren Sachstand enthalten und kann proaktiv oder auf Anfrage herausgegeben werden. Wichtigstes Ziel in dieser Phase ist das Unternehmen als aktiven Ansprechpartner zu etablieren, um die Kommunikationshoheit sicherzustellen und Gerüchte zu vermeiden.

Während parallel die wichtigsten Fragen und Antworten aufbereitet werden, sorgt das Kommunikations-Team dafür, dass sämtliche Kontaktpersonen des Unternehmens nach innen und außen – zum Beispiel im erweiterten Management, im Kundenservice oder im Vertrieb – das Holding Statement vorliegen haben und damit erste Anfragen beantworten können. So früh wie möglich sollte auch eine allgemeine interne Information folgen, die den Mitarbeitenden bei Bedarf Verhaltensregeln an die Hand gibt und zusätzlich Ansprechpartner im Kommunikationsteam für externe Anfragen nennt.

Nach Veröffentlichung einer Cyberattacke melden sich Mitarbeitende, Kunden, Journalisten und auch eine interessierte Öffentlichkeit mit unterschiedlichsten und teils sehr individuellen Fragen, dementsprechend müssen alle Touchpoints im Unternehmen so bald wie möglich Gesprächsleitfäden und FAQs bekommen, die kontinuierlich aktualisiert werden. Sie müssen zudem den Eskalationsprozess für besondere Anfragen kennen und diesen idealerweise trainiert haben.

Konsistenz und Kontinuität in der Kommunikation

Nach der zügigen ersten internen und externen Information sind Kontinuität und Konsistenz in der nächsten Phase Prioritäten für die Kommunikation. Die Forensik wird jetzt unter Umständen bereits einen besseren, wenn auch noch nicht abschließenden Blick auf die Situation haben. Nicht selten bringt diese Phase Erkenntnisse, die die erste Einschätzung noch einmal verändern – hier zeigt sich, wie wichtig es ist keine ungesicherten Infos herauszugeben oder Vermutungen zu formulieren.

In dieser Phase geht es darum Schritt für Schritt weitere verfügbare Informationen zur Verfügung zu stellen und einen angemessenen Dialog mit den jeweiligen internen und externen Zielgruppen aufzubauen. Mitarbeitende sollten über Intranet, Townhall- oder Teammeetings informiert werden. Wichtig ist hier nochmal eine Hilfestellung zum Umgang mit externen Anfragen oder Konversationen im persönlichen Umfeld, offline oder online sowie eine Social Media Policy zu geben. Kontinuierliches Monitoring von Print-, Online- und sozialen Medien hilft die korrekte Coverage der Fakten im Blick zu behalten und Spekulationen oder missverständliche Formulierungen rechtzeitig korrigieren zu können.

Schutz & Prävention

Längst schon geht es nicht mehr um die Frage, ob ein Unternehmen zum Opfer eines Cyberangriffs wird, sondern wann. Einen Notfallplan zu haben ist daher für jedes Unternehmen Pflicht. Die gute Nachricht ist, dass eine Vorbereitung auf die Bewältigung eines Cyberangriffs möglich ist. Für eine Prävention empfiehlt sich:

- Die Erstellung eines Incident-Response-Plans, der Zuständigkeiten, Aufgaben und Ansprechpartner in den Abteilungen des Unternehmens benennt inklusive einer guten und sorgfältigen Kommunikation.
- Allein schon aus Respekt gegenüber eigenen Teams und externen Zielgruppen ist eine gute und sorgfältige Kommunikation Pflicht: Anerkennen des Vorfalls (ohne verfrühtes Schuldeingeständnis), Begleitung des Krisenmanagements mit angemessenen Updates, Sichtbarkeit des CEO, verständliche Informationsschreiben, Aufzeigen von Learnings.
- Wenn es gelingt zu verdeutlichen, dass die Aufgabe ernst genommen wird, kann das Unternehmen eine Attacke nicht nur ohne größeren Reputationsschaden überstehen, sondern gestärkt daraus hervor gehen.
- Regelmäßige Übungen und Simulationen verschiedener Arten von Cyberangriffen und die notwendigen Maßnahmen zur Abwehr. Besonders sogenannte „Table-Top Exercises“ für technische Teams und auch für Manager haben sich als besonders effektiv erwiesen.
- Die Auswahl eines geeigneten *Incident-Response-Teams*, das über einen „Retainer“ genannten Vertrag kurze Reaktionszeiten und eine 24x7x365-Bereitschaft garantiert.
- Der Abschluss einer Cyberversicherung, die zumindest einen Teil der enormen Kosten übernimmt, die bei einem Cyberangriff entstehen können.

Über die Autoren

Dr. Hauke Hansen

ist Rechtsanwalt und Experte für Cybersicherheit, IT-Recht und Datenschutz. Er entwirft CyberSecurity-Strategien, um Unternehmer und Unternehmen vor Cyberattacken zu schützen und leistet ihnen Erste-Hilfe im Falle eines Cyberangriffs.

Robin Brocks

leitet das Incident Response Team von CrowdStrike für Europa, Afrika und dem Nahen Osten. Mit knapp 25 Jahren relevanter Berufserfahrung u.a. bei Lufthansa, Microsoft, Cisco und anderen großen Unternehmen ist er auch als Gutachter für IT-Forensik tätig. Er ist Reservist in der Digitalen Reserve der Bundeswehr und unterstützt auch hier gegen digitale Angriffe auf kritische Infrastrukturen.

Suntka von Halen

ist Director bei der Brunswick Group und Spezialistin für Restrukturierungs-, Krisen- und Veränderungskommunikation sowie Unternehmenspositionierung. Sie verfügt über langjährige Erfahrung in Beratung und auf Unternehmensseite und berät Kunden in internationalen Kommunikationsprojekten zu strategischen Fragen und in kritischen Situationen. Innerhalb von Brunswick's Cybersecurity-Praxisgruppe arbeitet sie als Co-Lead für Mandate in den Bereichen Crisis Preparedness und Crisis Response.

DATENSICHERHEIT – DILETTIEREN ODER DELEGIEREN?

Dr. Niels Lepperhoff

Einleitung

Art. 32 DS-GVO wirkt wie ein Fremdkörper in der Arbeit eines Datenschutzbeauftragten (DSB). Die übrigen Artikel sind vordergründing juristisch ausgerichtet. Art. 32 DS-GVO beschäftigt sich offenkundig mit purer (Informations-)Technik. Dank seiner einfachen Ausgestaltung und unkonkreten Vorgaben bleibt dem Betrachter der eigentliche Sprengsatz dieses Artikels für die Arbeit als DSB – wie vielfach zu beobachten – verborgen. Grund genug im Folgenden hinter die Kulissen zu schauen.

Die Lage ist komplex

Im Kern beschäftigt sich Art. 32 Abs. 1 DS-GVO mit technischen und organisatorischen Sicherheitsmaßnahmen, um personenbezogene Daten gemäß der genannten vier Schutzziele zu sichern. Sowohl Unternehmen als auch Behörden, Parteien und alle anderen Verantwortlichen i. S. d. Art. 4 Nr. 7 DS-GVO stellen komplexe Systeme dar, in denen zahlreiche technische Geräte und Programme unterstützt von oder gestört durch Mitarbeiter zusammenwirken. Dazu kommen verschiedene technische und organisatorische Schnittstellen nach draußen. Jedes Gerät, Programm und auch die Art und Weise der Bedienung beeinflussen die Sicherheit der verarbeiteten personenbezogenen Daten („IT-Sicherheit" im Folgenden).

Die Gesamtkomplexität des Systems hängt unter anderem von den folgenden Faktoren ab:

- Anzahl der Geräte
- Anzahl der Programme
- Anzahl der Schnittstellen nach außen
- Konfigurationsmöglichkeiten der Programme
- Güte der Softwareentwicklung bei den Herstellern der Programme und Geräte
- Manuelle Fehlerquellen in den Prozessen
- Fachliche Qualifikation der IT-Administratoren und Dienstleister
- Fachliche Qualifikation der Bediener hinsichtlich der korrekten Bedienung
- Anzahl der eingesetzten Software-as-a-Service-Anwendungen

Das IT-Sicherheitsniveau setzt sich folglich aus unzähligen kleinen Stellschrauben zusammen. Da (fast) jedes IT-Gerät und jedes Programm Auswirkungen auf die IT-Sicherheit hat sind diese alle in eine Betrachtung mit einzubeziehen.

Die Lage ist gefährlich

Ein sicheres IT-System bedeutet lediglich, dass bestimmte Angriffe keinen Erfolg haben. Es bedeutet nicht, dass jede Art von Angriff auf die Schutzziele keinen Erfolg hat. Bei der Prüfung von IT-Sicherheit und auch bei der Konzeption sind folglich die auf den Verantwortlichen wirkenden Gefahren und die möglicherweise eingesetzten Angriffstechniken zu berücksichtigen. Angriffstechniken entwickeln sich täglich weiter; angetrieben von mutmaßlichen Milliardengewinnen krimineller Gruppen und Aktivitäten staatlicher Akteure weltweit. Nordkorea steht beispielsweise im Verdacht 400 Millionen US-Dollar durch kriminelle Aktivitäten weltweit eingenommen zu haben.[1]

Zu dem Wissen um Angriffstechniken zählt nicht nur die Funktionsweise von Schadsoftware, sondern auch die Wirkungsweise von Fehlern in Software.[2] Da fast jeder Verantwortliche Websites betreibt und teilweise auch Funktionen programmiert oder durch Dienstleister programmieren lässt, besteht die Notwendigkeit sich mit fehlervermeidender Softwareentwicklung zu beschäftigen.

[1] Heise Online (2022): Nordkorea erbeutete 2021 angeblich fast 400 Millionen US-Dollar in Kryptogeld. 17.01.2022, URL: https://www.heise.de/news/Nordkorea-erbeutete-2021-angeblich-fast-400-Millionen-US-Dollar-in-Kryptogeld-6328901.html

[2] Bsp.: OWASP Top 10, URL: https://www.synopsys.com/glossary/what-is-owasp-top-10.html

Die Misere: Unzureichende Qualifizierung

Auf der Angreiferseite agieren hochprofessionelle Akteure, die weltweit arbeitsteilig vorgehen und teilweise über erhebliche finanzielle und personelle Ressourcen sowie vor Verfolgung sichere Rückzugsräume verfügen. Verantwortliche werden von teilweise kaum ausgebildeten und regelmäßig überlasteten IT-Administratoren verteidigt.

„Kaum ausgebildet" klingt hart. Doch muss man sich vor Augen führen, dass Jedermann den Beruf oder die Tätigkeit eines IT-Administrators ausführen darf. Eine Fachkunde oder deren Nachweis wird nicht verlangt. Ein Arzt muss seine Fachkunde nachweisen. Der IT-Administrator des Krankenhauses nicht, obwohl seine Fehler ebenfalls die Gesundheit der Patienten gefährden können. Das gleiche gilt für Entwickler von Software.

Um die eingangs skizzierte Komplexität zu erfassen und zu gestalten, bedarf es eines Studiums der Informatik (Master), da dort die notwendigen Techniken vermittelt werden. Strenggenommen ist anschließend oder begleitend eine Zusatzqualifikation in IT-Sicherheit erforderlich. Ich lade Sie ein: schauen Sie sich in Ihrem Umfeld die Qualifikationen der Softwareentwickler und IT-Administratoren an. Wieviel Prozent davon haben ein Informatikstudium absolviert oder – für die Nicht-Leitungspositionen und nicht mit Konzeptionierung betrauten Positionen – eine abgeschlossene Ausbildung passend zur Tätigkeit? Die vielfach unzureichende Qualifikation macht vor Dienstleistern nicht halt. Die Erfahrung zeigt, dass IT-Dienstleister, die die „IT" für ihre Kunden betreuen sollen, zudem mehr Wert auf geringe Wartungsaufwände als auf eine „sichere" Konfiguration legen. Selbst wenn der Kunde „Sicherheit" beauftragen will, besitzt längst nicht jeder Dienstleister die erforderliche Qualifikation eine „IT" sicher zu konzipieren.

Das wäre zu verkraften, wenn andere Personen und Funktionen in der Organisation sich für IT-Sicherheit zuständig sähen oder aktiv dazu beitragen würden. Die Erfahrung lehrt regelmäßig das Gegenteil. IT-Sicherheit wird der IT-Administration zugeschoben. Das gilt auch für Führungskräfte.

Ein Sicherheitskonzept bedarf immer auch der Mitarbeit des Verantwortlichen, da der Dienstleister selten für alle Programme und Geräte zuständig ist (Software as a Service!) und auch die Unternehmensabläufe meistens nicht kennt. Hier kommen wir zur regelmäßig fehlenden Fachkunde von Geschäftsführern, was IT-Sicherheit eigentlich bedeutet, und zur fehlenden Bereitschaft dafür Geld auszugeben. Selten wird bei der Beschaffung von Hard- und Software analysiert, welche Auswirkung die Beschaffung auf das Sicherheitsniveau hat.

Bye-bye Mythen

„Sicherheit muss einfach sein"

Komplexität weckt unweigerlich den Wunsch nach Vereinfachung. Dieser Wunsch findet seinen Verbündeten in der Geschäftsführung (geringe Kosten) und den Anwendern (freier Fluss der Daten ohne Hindernisse und Einschränkungen). So wird bspielsweise propagiert, dass für kleine Unternehmen geringere Sicherheitsanforderungen gelten müssten. Kleine Unternehmen können ihre Sicherheitskomplexität einfacher als große Unternehmen senken, wenn sie die geschilderten Komplexitätsfaktoren soweit wie möglich senken. Gleichwohl bleibt eine Mindestkomplexität übrig, die höher sein kann, als der Geschäftsführung lieb ist. Doch das ist mit Blick auf Art. 32 Abs. 1 DS-GVO vom Gesetzgeber gewollt, da auch kleine Unternehmen die Rechte und Freiheiten der Betroffenen „bedrohen".

„TOM-Listen prüfen reicht"

Wir kennen alle die Anlage „technische und organisatorische Maßnahmen" bei einer Auftragsverarbeitungsvereinbarung (AVV). Mehr oder weniger willkürlich werden in Stichpunkten „Sicherheitsmaßnahmen" aufgeführt, damit sich der Leser vom Sicherheitsniveau überzeugen kann. Diese Listen erlauben grundsätzlich keine Aussage – und damit auch keine Prüfung – des Sicherheitsniveaus.

29

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

Der BSI-Grundschutz dokumentiert die Risikoanalyse in Kurzform, nimmt aber nicht die Betroffenen nach Art. 32 DS-GVO in den Blick.

Download Broschüre "Informationssicherheit mit System" des Bundesamts für Sicherheit in der Informationstechnik

Typisches Beispiel aus der Praxis:

In einer AVV findet sich der Eintrag „Rechte- und Rollenmanagement". Nähere Ausführungen fehlen. „Alle Mitarbeiter dürfen mit Adminrechten auf alle Daten zugreifen" ist genauso ein „Rechte- und Rollenmanagement wie „nur zwei Personen haben Adminrechte und die übrigen dürfen nur auf die Daten zugreifen, die sie für ihre Arbeit brauchen". Welche Deutung zutrifft, lässt der Auftragsverarbeiter offen.

Noch deutlicher wird es, wenn man den Virenscanner betrachtet. Zur sachgerechten Beurteilung müsste der Leser wissen, an welchen Stellen der Datenflüsse welche Scanner (Hersteller, Version) mit welchen Updateintervallen (alle 5 Minuten oder 1 mal im Monat) installiert sind. Weiterhin müsste ausgeführt werden, was bei einem Alarm passiert und wie sichergestellt wird, dass Geräte ohne aktuelle Signaturen der Virenscanner nicht auf Programme zugreifen oder sich im Netz anmelden können.

TOM-Listen haben unbestritten den Vorteil, dass sie ein (falsches) Sicherheitsgefühl einfach dokumentieren können. Sie bieten zudem die Möglichkeit, nach Schlagworten wie „Rollen- und Rechtkonzept" zu suchen ohne sich fachlich mit der Angemessenheit der Maßnahme auseinandersetzen oder sich in die Tiefen der Ausgestaltung begeben zu müssen.

Wer das Sicherheitsniveau eines Dienstleisters prüfen will, braucht dessen Sicherheitskonzept i. S. d. Art. 32 DS-GVO. Nur so lässt sich beurteilen,

- ob die betrachteten Gefahren aus Sicht des Auftraggebers vollständig sind und
- ob die Maßnahmen alle identifizierten Gefahren und Risiken abdecken.

Der Versuch von Auftragsverarbeitern ihr Sicherheitskonzept als vertraulich einzustufen, um eine Nichtherausgabe zu begründen, kollidiert mit der sachlichen Notwendigkeit. Inhaltlich lässt sich ein Sicherheitskonzept so aufbauen, dass der Auftraggeber bei Einsichtnahme keine Kenntnis über sicherheitsrelevantes Wissen wie IP-Nummernkreise erfährt, aber alle für seine Beurteilung erforderlichen Angaben bekommt.

DSB als rettender Held?

Die Fortbildungszeit eines DSB ist begrenzt. Da er seine Fachkunde in allen Bereichen des Datenschutzrechtes aufrecht erhalten muss, wird sein Geld- und Zeitbudget bereits durch das Studium von Urteilen, juristischen Fachbeiträgen und dem Besuch der juristisch oder organisatorisch orientierten Fortbildungen beansprucht. Auf der anderen Seite ist das Feld der IT-Sicherheit – wie geschildert – hoch komplex, das heißt, der Fortbildungsbedarf (alle beim Verantwortlich eingesetzten Produkte, deren Konfigurationsmöglichkeiten, Angriffsweisen, Gefahren, eingesetzte Protokolle usw.) ist ebenfalls erheblich. Es erscheint deshalb regelmäßig unmöglich in beiden Feldern sattelfest im Detail zu sein.

Ein Weg vorwärts

Art. 32 Abs. 1 DS-GVO zeigt einen Weg auf. Im Kern verlangt Abs. 1 die Erstellung eines Sicherheitskonzepts, das eine Analyse der Gefahren, die aus der Kombination von Gefahr und ergriffenen Maßnahmen ermittelten Risiken sowie die betrachteten (oder noch zusätzlich ergriffenen) Maßnahmen umfasst.[3] In dem Konzept sind für jede Gefahr die Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit) zu betrachten sowie grundsätzlich alle Rechte und Freiheiten betroffener Personen in den Blick zu nehmen. Eine solche systematische Betrachtung erlaubt zudem mit Blick auf die Rechenschaftspflicht i. S. d. Art. 5 Abs. 2 DS-GVO darzulegen, dass die Betrachtung vollständig ist. In der Praxis bietet es sich an dabei auf Standards zurückzugreifen, die (auch) Konfigurationsanforderungen für konkrete Produkte umfassen.[4]

[3] Ausführlich dargestellt: Lepperhoff (2016): Datenschutz-Grundverordnung: Am Anfang steht das Sicherheitskonzept, IT-Sicherheit 04/2016, S. 58-61

[4] Bspw. BSI-Grundschutz-Kompendium, BSI Technische Richtlinien

[5] Da die Risikoanalyse des BSI-Grundschutz nicht die Betroffenen in den Blick nimmt, ist sie im Lichte von Art. 32 DS-GVO zu überprüfen.

[6] Lepperhoff (2016): Datenschutz-Grundverordnung: Am Anfang steht das Sicherheitskonzept, IT-Sicherheit 04/2016, S. 60

Diese Anforderungen helfen Administratoren und DSB zu erkennen, was konkret bei einem Produkt einzustellen ist. Fehlende Fachkunde lässt sich so – in Grenzen – kompensieren.

Es ist dabei darauf zu achten, dass die eingesetzten Standards oder Checklisten aus anderen Quellen auf einer nachvollziehbaren Risikoanalyse beruhen.

Andernfalls ist diese nachzuholen und die Checkliste gegen das Ergebnis zu validieren. Der BSI Grundschutz dokumentiert die Risikoanalyse in Kurzform in seinen Bausteinen.[5] Da für die Verarbeitung personenbezogener Daten grundsätzlich mindestens von „normalem" Schutzbedarf auszugehen ist, sind alle Anforderungen der Stufen „Basis (B)" und „Standard (S)" umzusetzen. Zusätzlich stellt das BSI Checklisten auf Basis des Grundschutz bereit, die eine strukturierte Erfassung des Umsetzungsgrads erlauben. Diese Checklisten sind im Zusammenspiel mit dem jeweiligen Baustein zu lesen, der weitere Erläuterungen und Hintergrundinformationen enthält.

Der BSI-Grundschutz kennt nur die Schutzziele „Vertraulichkeit", „Integrität" und „Verfügbarkeit". Das vierte Ziel „Belastbarkeit" (Art. 32 Abs. 1 lit. b) DS-GVO) fehlt. Versteht man „Belastbarkeit" („resilience") als Fähigkeit mit unvorhergesehenen Ereignissen umzugehen, dann wird deutlich, dass es sich nicht um ein Schutzziel im eigentlichen Sinn handelt, sondern um eine Eigenschaft des „Organismus Unternehmen".[6] Der BSI Grundschutz lässt sich folglich anwenden.

Iterativ vorgehen

Da der BSI-Grundschutz auf die eingangs geschilderte Komplexität reagiert, fällt er umfangreich aus. Hier kommt dem DSB das Prinzip Plan-Do-Check-Act der DS-GVO zupass. Er kann die Erfassung des Ist-Zustands, die konzeptionelle Gestaltung und die Prüfung der Umsetzung als iterativen Prozess umsetzen.

Eine Möglichkeit zur Ist-Erhebung ist beispielsweise monatlich drei Checklisten des Grundschutzes an einen Administrator zu senden. Dieser hat daraufhin drei Wochen zur Antwort Zeit. Der DSB wertet alle sechs Monate die Antworten aus und berichtet der Geschäftsführung über den Anteil der umgesetzten Maßnahmen im Vergleich der nach Grundschutz umzusetzenden Maßnahmen. Jede nicht umgesetzte Maßnahme erhöht grundsätzlich die Risiken für Betroffene und für das Unternehmen.

Jährlich könnte eine Beurteilung von DSB und IT-Administrator stattfinden, in der die Lücken fachlich bewertet werden. Zur fachlichen Bewertung zählen

- ob die durch die nicht umgesetzte Maßnahme entstehenden Risiken durch andere Maßnahmen kompensiert werden und
- wie hoch die zusätzlichen Risiken sind.

Fazit: Hilfe holen

Mittelfristig lohnt es sich auf die Einrichtung eines IT-Sicherheitsbeauftragten (oder Informationssicherheitsbeauftragten) hinzuwirken, der den DSB unterstützt und die IT-Sicherheit beim Verantwortlichen weiterentwickelt.

Über den Autor

Dr. Niels Lepperhoff

Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (einem Gemeinschaftsunternehmen des BvD e.V. und der GDD e.V.).

29

PRIVACYSOFT

Datenschutzmanagement as a Service

DATENSCHUTZ CAMPUS

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

WARUM SICH DATENSCHÜTZER MIT DETAILS BEIM CLOUD-COMPUTING AUSEINANDERSETZEN MÜSSEN

Eberhard von Faber

Datenschutz basiert auf IT-Sicherheit. Sie stützt sich auf die Datensicherheit, die durch Maßnahmen der IT-Sicherheit erreicht wird. Die Cloud ist kein abstraktes, virtuelles Gebilde. Sie besteht aus IT-Systemen die in Rechenzentren untergebracht sind und entsprechend abzusichern sind. Die Nutzung von Cloud-Computing-Services reduziert die Komplexität der IT und ihrer Absicherung für die Anwenderorganisation. Doch gleichzeitig wirft die Cloud neue Fragen auf, denen sich Datenschutz- und Datensicherheitsexperten stellen müssen. Die vielen Varianten und Modelle stellen Herausforderungen dar, die oft unterschätzt werden. Dieser Beitrag gibt eine Übersicht.

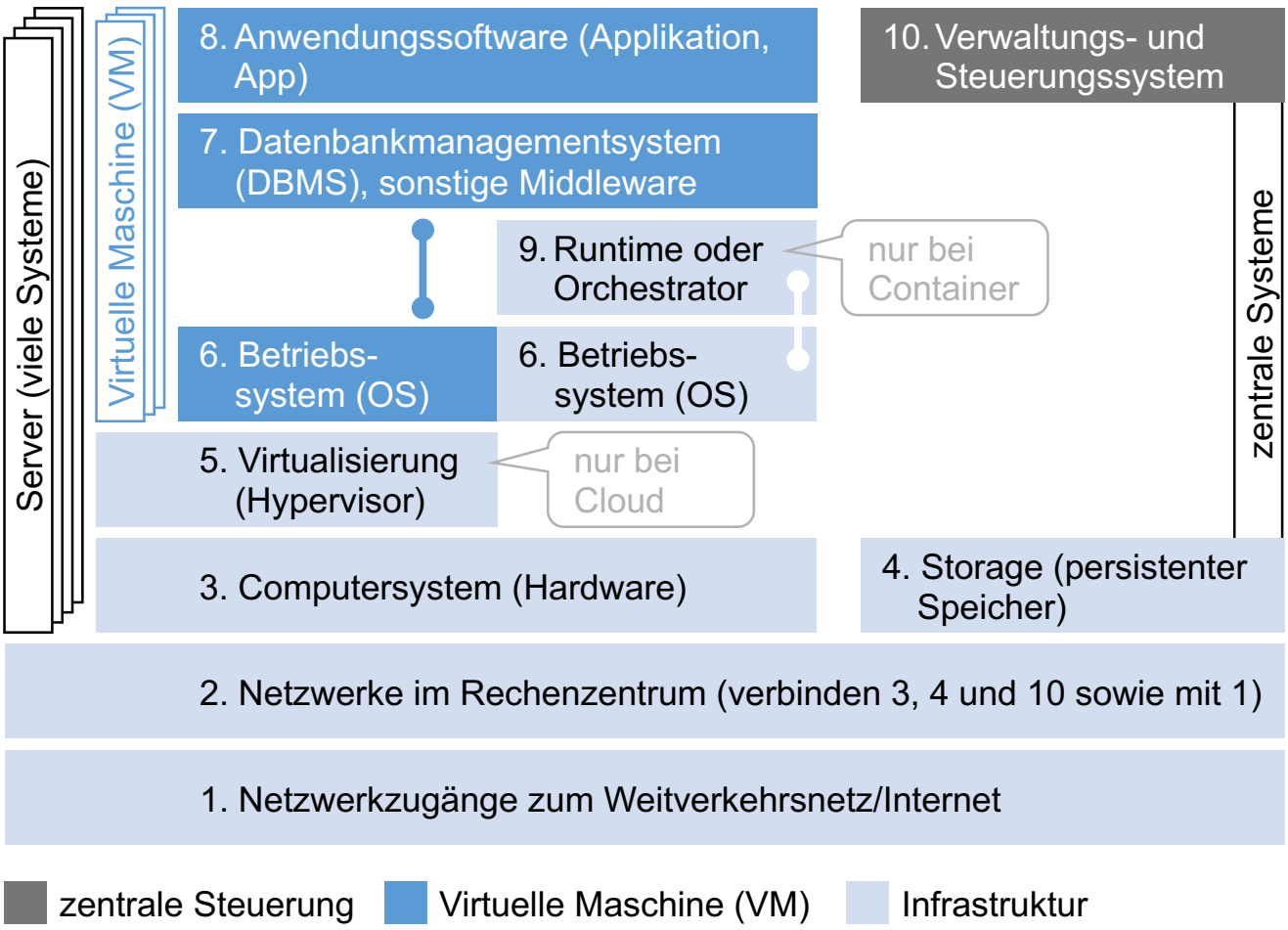


Abbildung: Grundsätzlicher Aufbau einer Cloud mit vielen Servern, auf denen jeweils mehrere Virtuelle Maschinen (VM) laufen können. Außerdem erkennbar ist die Struktur einer Infrastruktur mit Containern.

Was ist eine Cloud und was sind Container?

Grundsätzlich ist eine „Cloud“ eine Ansammlung vieler Computersysteme, die miteinander verbunden sind und zentral gesteuert werden. Die ungefähre technische Struktur ist wichtig für das Verständnis, welche Maßnahmen der IT-Sicherheit notwendig sind und was sie bewirken können. Die Rechentechnik im Rechenzentrum ist in Schichten aufgebaut, die einen IT-Stack (Stapel) bilden, den wir etwas erweitern (siehe Abbildung). Es handelt sich um eine implementierungsnahe Darstellung, die diverse Fachbegriffe benutzt. Als Referenz für die tägliche Arbeit wird ein unlängst erschienenes Lexikon [1] empfohlen. Es liefert verständliche Erklärungen von Begriffen und Zusammenhängen in der IT und der IT-Sicherheit und weitere Details.

Im Folgenden geht es zunächst um den grundsätzlichen Aufbau.

Die Schichten 1 bis 5 gehören zur Infrastruktur im engeren Sinne. Die Schichten 6 bis 8 bilden die Arbeitslast (workload), die in der Cloud „Virtuelle Maschine (VM)“ heißt. Die Infrastruktur ist der Gastgeber (host), die Virtuellen Maschinen (VM) die Gäste (guest).

Eine Cloud ist mandantenfähig und skalierbar. Das heißt, mehrere Anwender oder Anwenderorganisationen teilen sich eine Infrastruktur. Das bedeutet, dass die IT-Komponenten der Infrastruktur die Daten unterschiedlicher Anwender verarbeiten. Mehrere Virtuelle Maschinen (VMs) können sich einen physischen Computer teilen.

Damit das funktioniert, gibt es eine Virtualisierungsschicht (5), die jeder Anwendungssoftware oder VM die jeweils benötigten Ressourcen (Rechen-, Speicher- und Netzwerkkapazität) zur Verfügung stellt. Clouds optimieren die Ressourcennutzung und erreichen eine hohe Skalierbarkeit. Die zugeteilten Systemressourcen können bei höheren Leistungsanforderungen einfach und schnell wachsen und entsprechend auch schrumpfen.

Die Steuerung der Gastsysteme und VM erfolgt durch ein Cloud-Management-System (10). Dabei handelt es sich um eine Applikation, die direkten Zugriff auf die Virtualisierungsschicht (5) und den Storage (4) hat, sodass man VM (6 bis 8) aufsetzen, starten, verwalten und stoppen kann. Die Anwendungssoftware (Applikation, 8) kann über mehrere Computersysteme und Clouds verteilt sein.

Neben der Cloud gibt es Container-Lösungen. Bei ihnen steht die Kompatibilität und Portabilität im Vordergrund. Die Gastsysteme, die hier Container heißen (7 bis 8), können also auf verschiedenen Infrastrukturen (1 bis 4 plus 6) ausgeführt werden, auch mehrere Container auf einem System. Sie teilen sich dann das Betriebssystem (6) beziehungsweise dessen Kern. Das Betriebssystem beziehungsweise eine Erweiterung desselben verwaltet die Container (7 bis 8) und weist ihnen Ressourcen der Infrastruktur zu.

Anwendungen können aus sogenannte Microservices zusammengesetzt sein, die auf verschiedenen Systemen und eventuell sogar in verschiedenen Rechenzentren ausgeführt werden. Dazu wird eine Zwischenschicht (9) benötigt. Die hohe Abstraktion (Standardisierung der Infrastruktur aus Sicht des Gastsystems) ermöglicht die softwaregesteuerte Konfiguration und Bereitstellung der Infrastruktur („Infrastructure-as-Code“), was die Portabilität weiter erhöht und die Bereitstellung vereinfacht.

Eine Container-Lösung (9) kann auf einer Cloud-Infrastruktur (1-5) laufen. Dies vereint dann eine hohe Skalierbarkeit mit hoher Portabilität. Diese Ausführungen lassen erahnen, dass die IT mit der Cloud nicht etwa einfacher geworden ist. Vielmehr wird die Verantwortung für die Bereitstellung der IT-Services auf einen Cloud-Service-Provider verlagert. Das Gleiche gilt für die IT-Sicherheit. Doch die Verantwortung für die Daten und die Geschäftsabläufe, die mit der Cloud unterstützt werden, verbleibt bei der Anwenderorganisation, die den Provider beauftragt.

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

Wie kann man potenziell unsichere Cloud-Services sichern?

Cloud-Services gelten oft als unsicher, weil man unsicher ist, wie sicher sie sind. Oft kommt dann die Frage auf, ob man Cloud-Services nutzen kann ohne dem Provider/Dienstleister (vollständig) zu vertrauen. Es wird von Verschlüsselung und anderen Maßnahmen gesprochen, die der Anwender ergreifen kann, um einen eventuell mangelnden Schutz nachträglich zu verbessern.

Die Daten der Anwenderorganisation werden primär von der Anwendungssoftware (8) verarbeitet. Dafür benötigt und nutzt sie Rechenkapazität (compute), Speicherkapazität (storage) und Netzwerkkapazität (network), die die Cloud-Infrastruktur bereitstellt. Oft wird die Datenverarbeitung von einem Nutzer angestoßen, dessen Computer über das Internet mit der Cloud verbunden ist. Anfrage und Daten fließen von dort in das Rechenzentrum (1), durch dessen Netzwerke (2) und von dort zu dem Computersystem (3), auf dem die Anwendungssoftware (8 mit 7) läuft.

Zwischen dem Computersystem (Hardware) und der Anwendungssoftware liegen ein Betriebssystem (6) und je nach Installation weitere Softwareschichten (5 und/oder 9). Die dauerhafte Datenspeicherung erfolgt im Storage-System (4). Das heißt, einzig die Einheit Verwaltung/Management (10) hat keinen direkten Kontakt mit der Speicherung und Verarbeitung der Daten des Anwenders.

Was können Anwender oder ihre Dienstleister außerhalb der Cloud tun, um ihre Daten in der Cloud zu schützen? Dafür gibt es diverse Möglichkeiten aber auch Grenzen. In Bezug auf den Schutz personenbezogener Daten zählen dazu verschiedene Formen der Maskierung (wie Anonymisierung und Pseudonymisierung), bei denen die personenbezogenen Originaldaten (vor der Übergabe an den Cloud-Service) durch andere ersetzt werden, und zwar so, dass die Datenverarbeitung (durch den Cloud-Service) nicht eingeschränkt ist und die gleichen Ziele erreicht werden.

Ein probates Mittel für den Schutz der Vertraulichkeit von Daten ist die Verschlüsselung, deren Einsatz jedoch schnell an Grenzen stößt. Wie bei allen Sicherheitsmaßnahmen muss man zunächst unterscheiden, wogegen sie schützen sollen. So kann der Cloud-Service-Provider die Datenbanken oder den Speicher (Storage) selbst verschlüsseln. In diesen Fällen können die benötigten kryptografischen Schlüssel vom Provider oder von der Anwenderorganisation verwaltet werden. Physisch liegen sie aber in der Cloud, das heißt, in einem Sicherheitsmodul (Software oder Hardware) im Rechenzentrum des Providers. Bei sogenannten Self-Encrypting Devices (SED) befindet sich der Schlüssel in der Steuerungseinheit der Festplatte im Storage. Derartige Maßnahmen schützen primär vor bestimmten Innentätern beim Provider sowie davor, dass Daten bei Wiederverwendung oder Verschrottung der Festplatte in unberechtigte Hände gelangen. Die andere Variante ist auch unter der Bezeichnung Cloud-Security-Gateway bekannt. Dabei handelt es sich um ein dem Cloud-Computing-Service vorgeschaltetes Computersystem, das Daten verschlüsselt (oder maskiert) bevor sie an die Cloud übermittelt werden und sie auf dem Weg zurück zum Anwender wieder entschlüsselt (oder demaskiert).

Für den Anwender ist der Cloud-Security-Gateway transparent („unsichtbar"). Er schützt vor allen Angreifern außerhalb der Anwenderorganisation also auch vor Problemen beim Cloud-Service-Provider.

Während die erstgenannte Variante (Verschlüsselung erfolgt in der Cloud) sehr effektiv und relativ einfach zu implementieren ist, gibt es bei der zweiten Variante mit umfassenderem

Schutzprofil (Verschlüsselung außerhalb der Cloud) starke Einschränkungen in der Anwendbarkeit. Die Einschränkungen rühren daher, dass die Daten in der Cloud meist auch verarbeitet werden sollen. Das funktioniert mit verschlüsselten Daten nicht. Formatvorgaben verhindern oft schon das Speichern von verschlüsselten Daten in Feldern. Möglich ist dagegen die Nutzung der Cloud als Speicher von Dateien, Transaktionsdaten und dergleichen. In diesem Fall müssen jedoch sogar einfache Suchfunktionen außerhalb der Cloud nachgebildet werden. Lösungen wie CASB (Cloud Access Security Broker) sind ebenfalls dem Cloud-Computing-Service vorgeschaltet, übernehmen aber, je nach Implementierung, neben der Verschlüsselung und Maskierung von Daten weitere Sicherheitsfunktionen wie Authentisierung, Autorisierung und den Schutz vor Malware.

Wo passieren die Fehler, was muss implementiert werden?

Die IT einer Cloud ist komplex und die für ihre Absicherung notwendigen Maßnahmen sind es nicht minder. Auch wenn für viele Sicherheitsmaßnahmen nur der Cloud-Service-Provider sorgen kann, bleibt, und das wird häufig vergessen, einiges der Anwenderorganisation überlassen.

Gerade für den Datenschutz spielen die Service-Architektur, die Anwendungssoftware und das Datenhaltungskonzept eine entscheidende Rolle. Handelt es sich nicht gerade um „Software-as-a-Service“ (der Provider stellt auch die Gastsysteme), so sind diese Komponenten nicht Teil des Cloud-Services, sondern werden von der Anwenderorganisation bestimmt bzw. geliefert. Das gleiche gilt beispielsweise meistens auch für das Service Continuity Management einschließlich Backup und Recovery. Auch für diese Komponenten ist die Anwenderorganisation verantwortlich.

Es verwundert bei einem komplexen System wie einer Cloud kaum, dass die wichtigste Herausforderung bezüglich der IT-Sicherheit darin besteht, für Vollständigkeit und das richtige Zusammenspiel aller Komponenten zu sorgen. Die Frage der Vollständigkeit ist wichtig und einer der Gründe, auf diverse Cloud-Sicherheitsstandards wie zum Beispiel [2], [3] und [4] zurückzugreifen.

Zusammenwirken: Um den eigentlichen Cloud-Computing-Service zu nutzen, müssen bereits verschiedenste Entscheidungen getroffen und die entsprechenden Einstellungen korrekt vorgenommen werden. Doch der Cloud-Service-Provider stellt nicht nur den eigentlichen Cloud-Computing-Service mit diversen Optionen bereit, sondern zusätzlich weitere optionale Komponenten oder Dienste zum Beispiel für das Identitäts- und Zugriffmanagement (IAM), für die Verwaltung von Software-Images und die Überwachung (Monitoring, Dashboard). Auch diese sind für die IT-Sicherheit relevant. Sie müssen ebenfalls ausgewählt, konfiguriert und integriert werden. Auch bei führenden Cloud-Anbietern werden die Anwenderorganisationen damit meistens allein gelassen. Das IT-Beratungsunternehmen Gartner sagte aber bereits 2015 für die nächsten fünf Jahre voraus, dass etwa 95 Prozent der Sicherheitsmängel durch die Partei verursacht werden, die den Cloud-Service einrichtet und konfiguriert. Deshalb bieten Cloud-erfahrene Dienstleister wie T-Systems inzwischen Hilfe an und unterstützen Anwenderorganisationen bei der Einrichtung und Konfiguration firmenfremder Cloud-Computing-Services.

Doch die Liste der benötigten Zusatzleistungen für die eigentlichen Cloud-Services ist noch länger: Die IT-Systeme und die IT-Sicherheit müssen gepflegt werden. Die Cloud-Services müssen betrieblich überwacht werden, um Ausfälle und sicherheitsrelevante Sachverhalte frühzeitig erkennen und rechtzeitig bearbeiten zu können. Dies betrifft auch die Erkennung und Behandlung möglicher Datenschutzvorfälle.

Die allermeisten Cloud-Services bieten dafür allenfalls Werkzeuge (IT-Tools). Nur bei vollständig verwalteten („gemanagten“) Cloud-Services übernimmt der Provider alle Tätigkeiten und führt sie im Auftrag von und speziell für die Anwenderorganisation aus. Auch führende Cloud-Service-Provider überlassen viele Verwaltungs- beziehungsweise Managementaufgaben regelmäßig Anwendern, Partnern und Fremdfirmen, oder bieten sie separat als optionale Zusatzleistung an.

Die eher personalintensiven Aufgaben der Einrichtung und Konfiguration der Cloud-Services einerseits und der Verwaltung, Überwachung und Nachsteuerung andererseits sind essentiell für die

Einhaltung von Anforderungen (Compliance) und ein adäquates Niveau der Datensicherheit und des Datenschutzes. Diesbezügliche vertragliche Regelungen und Zusagen können nur auf Basis vorhandener Management-Aktivitäten gemacht werden, die mit der betrieblichen Praxis der Anwenderorganisation verzahnt sind.

Es liegt nahe, dass es ein vollständiges Management eher bei individualisierten Cloud-Services für Unternehmen und größere Organisationen gibt als bei einem auf große Verbreitung zielenden Angebot für jedermann. Das bringt uns zur Unterscheidung der Cloud-Services nach der Form ihrer Bereitstellung (Deployment Model): Public-Cloud-Services sind Angebote, die von jedem über das Internet genutzt werden können. Die Nutzer, ganz gleich welcher Provenienz, teilen sich eine Infrastruktur. Private-Clouds und Virtual-Private-Clouds unterscheiden sich von Public-Clouds dadurch, dass die IT nur von einer Anwenderorganisation genutzt wird bzw. von einigen, als vertrauenswürdig eingestuften. Auch muss hier der Zugang nicht über das offene Internet erfolgen. Derartige Feinheiten haben ebenfalls Einfluss auf die IT-Sicherheit beziehungsweise das Risikoprofil, mindestens aber auf die Form der sicheren technischen Integration in die Geschäftsprozesse der Anwenderorganisation.

Wer ist wofür verantwortlich? Cloud-Unterschiede, Arbeitsteilung und Verantwortlichkeit

Die Kette ist so stark wie ihr schwächstes Glied. Aber wie sieht die Kette eigentlich aus? Wie wir gesehen haben, besteht die Cloud aus vielen IT-Komponenten. Sie wird mitunter mit Hilfe zusätzlicher Dienste abgesichert. Und alle Komponenten und Dienste müssen adäquat konfiguriert und verwaltet werden. Doch wer ist für welches Glied in der Kette verantwortlich? Sind die Kettenglieder nahtlos miteinander verbunden? Sind Verantwortlichkeiten klar zugeordnet und werden sie adäquat wahrgenommen, sodass ein sicheres integriertes Ganzes entsteht? Viele Sicherheits- und Datenschutzvorfälle nehmen ihren Ursprung oder gewinnen Dramatik auch dadurch, dass zunächst nur auf die Inbetriebnahme beziehungsweise den „Day-1“ nach der Erstbereitstellung hingearbeitet wird. Aber wie andere IT sind auch Cloud-Services eigentlich nie fertig: Es werden Fehler gefunden, die ausgemerzt werden müssen. Die Anforderungen der Anwenderorganisation an die Cloud-Services ändern sich. Kapazitäten müssen angepasst, neue Funktionen implementiert und bestehende Funktionen modifiziert werden. Nicht zuletzt kommt es zu Vorfällen, die selbst oder deren Ursachen durch Überwachung und Analysen gefunden werden müssen. Diese Betriebsphase „Day-2“ (der Pflege und Modernisierung) muss ebenfalls vorbereitet werden. Wer muss dies tun? Und was muss konkret getan werden?

Es liegt in der Natur der Cloud-Angebote als Dienstleistung (IT-Service und nicht IT-Produkt!), dass es zu dem „Wer ist wofür verantwortlich?“ keine feststehenden Antworten gibt. Das gilt auch für hochstandardisierte Cloud-Services. Allen voran sind die Angebote der Marktführer meist keine Rundum-Sorglos-Pakete.

Zur Unterscheidung der Cloud-Angebote werden meist nur drei sogenannte Servicemodelle herangezogen (IaaS, PaaS und SaaS). In ihrer einfachen Form beschreiben diese Servicemodelle, welche Partei (Anwenderorganisation oder Cloud-Service-Provider) die IT-Komponenten bereitstellt und damit die Verantwortung für sie übernimmt. Bei IaaS (Infrastructure-as-a-Service) ist der Cloud-Service-Provider nur für die Infrastruktur (1-5 in der Abbildung) verantwortlich, bei PaaS kommen Plattformkomponenten (6-7) hinzu, bei SaaS werden alle IT-Komponenten vom Provider bereitgestellt (1-8).

Diese Einteilung ist nicht sehr detailliert. Problematischer ist aber, dass die Verwaltungs- beziehungsweise „Management“-Tätigkeiten wie Ressourcenverwaltung, Rechteverwaltung, Backup, Protokollierung, Überwachung und Änderung nicht näher betrachtet werden. Die Zuordnung muss man sich konzeptionell erst erarbeiten. Auf Seiten der Anwender wird also detailliertes Wissen über die IT und die IT-Sicherheit benötigt. Abhängig von der Zuweisung zum Beispiel von Wartungsaktivitäten werden unterschiedliche Zugriffsrechte und Zugriffsmöglichkeiten (Konnektivität) benötigt. Deshalb sollte man die Beschreibung der Servicemodelle erweitern [5]. Zudem wäre es sehr hilfreich, wenn deren Beschreibung in standardisierter Form erfolgen würde, damit

Verständlichkeit und Vergleichbarkeit gewährleistet sind [5]. Im weiteren Sinne sollte das Servicemodell also auch die Arbeitsteilung und Verantwortung bei der Implementierung und im Betrieb beschreiben – einschließlich der IT-Service-Management-Aktivitäten, wie sie in ITIL® und ISO/IEC 20000 beschrieben sind und mit oder ohne DevOps umgesetzt werden.

Bis dies Stand der Technik und gemeinsame Praxis ist, müssen sich Anwenderorganisationen in die beschriebenen Details selbst einarbeiten oder sich von einem weiteren IT-Dienstleister helfen lassen. Die IT ist mit der Cloud nicht viel einfacher geworden. Das Gleiche gilt für die IT-Sicherheit. Das meiste übernimmt zwar der Cloud-Service-Provider. Doch es gibt viele Betriebsmodelle, Optionen und Konfigurationen. Am Ende ist es die Anwenderorganisation, die von möglichen Ausfällen und Verstößen gegen Sicherheits- und Datenschutzrichtlinien betroffen ist. Sie trägt auch die Verantwortung für Folgeschäden, die ihre IT-gestützten Geschäftsprozesse verursachen. Es gibt Zusatzdienste wie die beschriebenen Cloud-Security-Gateways. Im Bereich „Privacy-Enhancing Computation (PEC)" (datenschutzverbesserndes Berechnen) werden neue Techniken entwickelt. Diese Lösungen können einen Teil der Datenschutzsorgen mindern. Aber auch sie müssen verstanden und sachgerecht eingesetzt werden.

Cloud-Services haben viele Probleme gelöst, aber zugleich eine Welt mit neuen Herausforderungen geschaffen. Die Industrialisierung der IT verlagert viele Aufgaben in das Liefernetzwerk. Doch gleichzeitig wird dadurch dessen Aufsicht und Kontrolle wichtiger. Noch hat die IT nicht die Qualität und Reife erreicht, dass sich Anwenderorganisationen auf die reine Beschaffung konzentrieren können. Sie sind mit ihren Datenschutz- und Datensicherheitsexperten immer noch Teil des Designs, der Implementierung und vieler Phasen im Betrieb der Cloud-Services [6].

Über den Autor

Prof. Dr. Eberhard von Faber

Technische Hochschule Brandenburg und T-Systems, beschäftigt sich mit Sicherheitsarchitekturen, Prozessen, der Standardisierung von IT-Sicherheit, den Anforderungen von Anwenderorganisationen und Fragen der Zusammenarbeit in Lieferketten.

▶ ESARIS@t-online.de

Literatur

[1] Eberhard von Faber: IT und IT-Sicherheit in Begriffen und Zusammenhängen, Thematisch sortiertes Lexikon mit alphabetischem Register zum Nachschlagen; Springer-Vieweg, 2021; ISBN 978-3-658-33430-7; https://doi.org/10.1007/978-3-658-33431-4

[2] Cloud Security Alliance (CSA): CSA Cloud Controls Matrix (CCM); Version 4, https://cloudsecurityalliance.org/research/cloud-controls-matrix/

[3] ISO/IEC 27017 - Informationstechnik - Sicherheitstechniken - Verhaltenskodex für Informationssicherheitskontrollen auf der Grundlage von ISO/IEC 27002 für Cloud-Services

[4] Cloud-Computing Compliance Controls Catalogue (C5:2020) des Bundesamts für Sicherheit in der Informationstechnik (Deutschland)

[5] Eberhard von Faber: Vorschlag zur Verbesserung von Cloud-Sicherheitsstandards; Berücksichtigung der unterschiedlichsten Service- und Bereitstellungsmodelle mit nur zwei Anforderungen; in: Datenschutz und Datensicherheit - DuD, 46, pp. 45-51. January 2022, Springer, ISSN 1614-0702, https://doi.org/10.1007/s11623-022-1559-x (frei verfügbar unter: https://rdcu.be/cEp9H)

[6] Eberhard von Faber und Wolfgang Behnsen: Joint Security Management: organisationsübergreifend handeln - Mehr Sicherheit im Zeitalter von Cloud-Computing, IT-Dienstleistungen und industrialisierter IT-Produktion; Springer-Vieweg, 2018, ISBN 978-3-658-20833-2. https://doi.org/10.1007/978-3-658-20834-9

DATENSCHUTZBEAUFTRAGTE UND AUFSICHTSBEHÖRDEN: CHANCEN UND GRENZEN DER ZUSAMMENARBEIT

Andrea Backer-Heuveldop, Dr. Bernd Schütze

In der Entstehungsgeschichte der DS-GVO wurde die in Art. 39 Abs. 2 lit. d und e DS-GVO verankerte Pflicht zur Zusammenarbeit zwischen Datenschutzbeauftragten und Aufsichtsbehörde sehr intensiv und kontrovers diskutiert.[1] Im ursprünglichen Entwurf der EU-Kommission hatte der Datenschutzbeauftragte noch die Aufgabe der „Überwachung der auf Anfrage der Aufsichtsbehörde ergriffenen Maßnahmen".[2] Nicht ohne Grund wurde diese von der EU-Kommission ursprünglich eher als Ausführungsorgan der Aufsichtsbehörde angelegte Aufgabe des Datenschutzbeauftragten im Rahmen der Trilog-Verhandlungen in Richtung gleichberechtigter Zusammenarbeit geändert[3], aus „to monitor the response to requests from the supervisory authority, […]" wurde im Rahmen der Trilog-Verhandlungen „to cooperate with the supervisory authority". Eine vertrauensvolle Zusammenarbeit zwischen Datenschutzbeauftragten und einer Unternehmensleitung ist nur möglich, wenn der Datenschutzbeauftragte bei der Wahrnehmung seiner aus der DS-GVO resultierenden Aufgaben auch seinen Treue- und Geheimhaltungsverpflichtungen gegenüber seinem Auftrag- oder Arbeitgeber nachkommen kann. Wie, in welchem Umfang und in welchen Fällen genau die Zusammenarbeit mit der Aufsichtsbehörde erfolgen soll und insbesondere an welchen Stellen sie ihre Grenzen findet, beschreibt die DS-GVO jedoch letztlich nicht. Daher werden diese Aspekte im Folgenden näher betrachtet.

Datenschutzbeauftragte als Anlaufstelle der Aufsichtsbehörden

Der Datenschutzbeauftragte ist nach Art. 39 Abs. 1 lit. d und e DS-GVO ganz allgemein zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet.[4] Es erscheint sinnvoll, dass der Datenschutzbeauftragte gemäß Art. 39 Abs. 1 lit. e DS-GVO als Anlaufstelle der Aufsichtsbehörde agiert, denn der Datenschutzbeauftragte ist wohl der fachlich anerkannteste Ansprechpartner der Aufsichtsbehörden beim Verantwortlichen oder dem Auftragsverarbeiter. So kann eine Verständigung von Fachexperte zu Fachexperte erfolgen, was die Kommunikation in der Regel deutlich vereinfacht.

Zudem ist der Datenschutzbeauftragte entsprechend Art. 38 Abs. 1 DS-GVO durch Verantwortliche beziehungsweise Auftragsverarbeiter „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen" einzubinden. Es darf also erwartet werden, dass Datenschutzbeauftragte in die Themen, die Aufsichtsbehörden ansprechen, sowieso eingebunden sind. Weiterhin berichten Datenschutzbeauftragte gemäß Art. 38 Abs. 3 S. 3 DS-GVO „unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters". Hier können Anliegen einer Aufsichtsbehörde direkt entsprechend adressiert werden. Dabei ist jedoch zu beachten, dass in der Praxis vielen Datenschutzbeauftragten ein ständiger und bedarfsgerechter Zugang entgegen den gesetzlichen Vorgaben zur höchsten Managementebene verwehrt wird. Dennoch kennen die Datenschutzbeauftragten das jeweilige Unternehmen in der Regel sehr gut und können mitunter ihrerseits die Aufsichtsbehörden beraten, wenn durch andere Ansprechpartner im Unternehmen als in der höchsten Managementebene Anliegen oder Fragen der Aufsichtsbehörden schneller bearbeitet werden können – auch dies spricht dafür, dass Datenschutzbeauftragte als Anlaufstelle agieren können.

Jedoch macht weder die Funktion als Anlaufstelle noch die Pflicht zur Zusammenarbeit den Datenschutzbeauftragten zum Hilfsorgan der Aufsichtsbehörde[4]. Datenschutzbeauftragte sind

[1] Klug C. (2016) Der Datenschutzbeauftragte in der EU - Maßgaben der Datenschutzgrundverordnung. ZD: 319

[2] siehe Art. 39 Abs. 1 lit. g DS-GVO-E, zu finden unter Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). Online, zitiert am 2022-01-18; verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A52012PC0011

[3] Regulation (EU) No XXX/2016 of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Online, zitiert am 2022-01-18; verfügbar unter https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/01/s_2014_2019_plmrep_COMMITTEES_LIBE_DV_2015_12-17_3_4column_table_EN.pdf

[4] So z. B.

- Drewers S.: Art. 39 Rn. 35. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7
- Kort M. (2017) Was ändert sich für Datenschutzbeauftragte, Aufsichtsbehörden und Betriebsrat mit der DS-GVO? ZD: 7
- Heberlein H.: Art. 39 Rn. 16. In: Ehmann/Selmayr (Hrsg.) Datenschutz-Grundverordnung. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-72006-2

dem jeweiligen Unternehmen, in welchem sie benannt sind, zugeordnet, sind integraler Bestandteil in der Organisation des Verantwortlichen oder des Auftragsverarbeiters. Datenschutzbeauftragte fungieren in ihrer Tätigkeit als Anlaufstelle der Aufsichtsbehörden deshalb als eine Art Intermediär, als Vermittler und Koordinator zwischen Unternehmen und Aufsichtsbehörde, insbesondere bei der Unterstützung der in Art. 31 DS-GVO vorgegebenen Zusammenarbeit zwischen Aufsichtsbehörde und Verantwortlichem oder Auftragsverarbeiter. Dabei gehören Datenschutzbeauftragte immer zur Sphäre des Verantwortlichen.[5] Dies wird auch vom EDSA so gesehen: Der Datenschutzbeauftragter ist „Mittler", heißt es in den Leitlinien der Artikel-29-Datenschutzgruppe.[6]

Mit der in der DS-GVO verankerten Funktionalität des Datenschutzbeauftragten als Anlaufstelle korrespondiert die in Art. 37 Abs. 7 DS-GVO verankerte Pflicht des Verantwortlichen der Aufsichtsbehörde die Kontaktdaten des Datenschutzbeauftragten mitzuteilen; nur wenn den Aufsichtsbehörden bekannt ist, wie ein Datenschutzbeauftragter zu erreichen ist, kann er als Anlaufstelle Aufsichtsbehörden genutzt werden. Insbesondere bei extern benannten Datenschutzbeauftragten müssen die Aufsichtsbehörde darauf achten einen Datenschutzbeauftragten in seiner jeweiligen Funktion beim jeweiligen Verantwortlichen beziehungsweise Auftragsverarbeiter anzusprechen: Nur weil die Kontaktdaten des einem extern benannten Datenschutzbeauftragten gehörenden Unternehmens seitens der Aufsichtsbehörde bekannt sind, wird durch diese Kenntnis nicht legitimiert diese Firmenkontaktdaten des Unternehmens des Datenschutzbeauftragten als Anlaufstelle für An- und Nachfragen bezüglich eines Unternehmens, bei dem der Datenschutzbeauftragte benannt ist, zu nutzen. Aber dies sollte für Aufsichtsbehörden eine Selbstverständlichkeit darstellen: Mandantentrennung gehört schon sehr lange zu den Grundpfeilern des Datenschutzrechts.

Dies gilt selbstverständlich auch für die externen Datenschutzbeauftragten, die dafür Sorge tragen sollten für die eigene, mandantenbezogene Kommunikation mit der Aufsichtsbehörde klare Rahmenbedingungen zu schaffen und dafür Kontaktdaten zu nutzen, die eine eindeutige Zuordenbarkeit zum Verantwortlichen beziehungsweise Auftragsverarbeiter ermöglicht. Ein Beispiel, um dies zu verdeutlichen:

> Z ist als externer Datenschutzbeauftragter für die Firma „xy" tätig und nutzt dabei für seinen Geschäftsbetrieb die eigene E-Mail-Adresse Z@privacy-gmbh.de. Zusätzlich richtet er in seiner eigenen Domäne einen Account dsb@privacy-gmbh.de für seine Mandanten ein. Eine Mail an dsb@privacy-gmbh.de für den Datenschutzbeauftragten der Firma „xy", welche für ihren Internetauftritt https://xy-gmbh.de und für ihre elektronische Kommunikation Mailadressen nach dem Schema vorname.nachname@xy-gmbh.de nutzt, ist für den externen Datenschutzbeauftragten der Firma „xy" nicht angemessen: der Verantwortliche hat einerseits keinen Zugriff auf den Mailserver der Firma „privacy-gmbh" des externen Datenschutzbeauftragten und kann somit eingehende Mails nicht im Rahmen der Vorgaben von Art. 32 DS-GVO durch technische und organisatorische Maßnahmen schützen, andererseits wird den Transparenzvorgaben der DS-GVO durch die Nutzung einer Mailadresse einer fremden Firma nicht entsprochen.

Anlaufstelle, aber nicht Annahmestelle

Wenngleich ein Datenschutzbeauftragter als Anlaufstelle für die Aufsichtsbehörden agiert, so handelt es sich bei ihm regelhaft nicht um eine Vertretung der Geschäftsführung des Unternehmens, welche den Datenschutzbeauftragten benannte. Auch wenn der Datenschutzbeauftragte das Unternehmen nach außen hin in Datenschutzfragen repräsentiert und insbesondere betroffene Personen entsprechend Art. 38 Abs. 4 DS-GVO ihn „zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte" zurate ziehen können, hat ein Datenschutzbeauftragter keine Vertretungsbefugnis und insbesondere ist ein Datenschutzbeauftragter kein Adressat eines Schreiben, welches eine Aufsichtsbehörde an das Unternehmen richtet. Dies gilt insbesondere dann, wenn der Erhalt dieses behördlichen Schreibens rechtliche Konsequenzen für ein Unternehmen wie beispielsweise den Beginn einer Frist beinhaltet.

[5] Heberlein H. (2019) Der Datenschutzbeauftragte – ein Kernelement der Datenschutz-Grundverordnung. jM: 25

[6] Artikel-29-Datenschutzgruppe: Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), Abschnitt 4.3. Zuletzt überarbeitet und angenommen am 5. April 2017, vom Europäischen Datenschutzausschuss bestätigt am 25. May 2018. Online, zitiert am 2022-01-18; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_de

Eine Vertreterfunktion, welche zwingend die Einnahme der Position des Unternehmens verlangt, ist grundsätzlich mit der in Art. 38 Abs. 3 S. 1 DS-GVO i. V. m. ErwGr. 97 verankerten Unabhängigkeit eines Datenschutzbeauftragten unvereinbar. Aus diesem Grund stellten die Aufsichtsbehörden fest, dass bei Personen des leitenden Managements wie etwa Leiter eines Unternehmens oder Leiter des operativen Geschäftsbereichs grundsätzlich von einem Interessenkonflikt auszugehen ist und Personen in dieser Position deswegen nicht zum Datenschutzbeauftragten benannt werden sollten. [7]

Datenschutzbeauftragte sind außerdem keine Empfangsvertreter entsprechend § 164 BGB, jedoch können Datenschutzbeauftragte mitunter als Empfangsboten anzusehen sein. Laut Bundesarbeitsgericht[8] ist Empfangsbote, „wer vom Empfänger zur Entgegennahme von Erklärungen ermächtigt worden oder nach der Verkehrsauffassung als ermächtigt anzusehen ist." Um entsprechend der Verkehrsauffassung als Empfangsbote zu gelten, muss laut BAG nicht nur „eine auf eine gewisse Dauer angelegte räumliche Beziehung zum Adressaten" vorhanden sein, sondern darüber hinaus eine persönliche oder vertragliche Beziehung zum Adressaten existieren.[9] Insbesondere intern benannte Datenschutzbeauftragte können aufgrund ihrer räumlichen Nähe, der aus dem Arbeitsvertrag resultierenden Beziehung sowie der aus Art. 38 Abs. 3 S. 3 DS-GVO resultierenden Möglichkeit, direkt der höchsten Managementebene zu berichten, als Empfangsboten anzusehen sein. Bei extern benannten Datenschutzbeauftragten dürfte regelhaft die fehlende räumliche Nähe eher dagegensprechen sie als Empfangsboten anzusehen.

Bei der Übergabe einer Willenserklärung an einen Empfangsboten kann „erst nach Ablauf der Zeit, die der Empfangsbote für die Übermittlungstätigkeit unter den obwaltenden Umständen normalerweise benötigt, erwartet werden, dass er von der Erklärung Kenntnis nehmen kann".[10]

Nur wenn ein Verantwortlicher den Datenschutzbeauftragten in einem speziellen Fall zur Annahme von behördlichen Schreiben ermächtigte (etwa weil die Kommunikation in diesem Fall grundsätzlich über den Datenschutzbeauftragten abgewickelt werden soll), kann eine Aufsichtsbehörde in diesem speziellen Einzelfall Schreiben einem Unternehmen über den Umweg der Einbeziehung des Datenschutzbeauftragten zukommen lassen.

Keine Pflicht zur Meldung von Verstößen

Hingegen besteht für Datenschutzbeauftragte keine Pflicht, die im Rahmen der aus Art. 39 Abs. 1 lit. b. DS-GVO resultierenden Überwachungsaufgabe durch ihn festgestellten und der Unternehmensleitung entsprechend Art. 39 Abs. 1 lit. a DS-GVO gemeldeten Verstöße auch den Aufsichtsbehörden zu melden, selbst wenn die Verstöße seitens des Verantwortlichen beziehungsweise Auftragsverarbeiters fortgesetzt werden.[11] Aber auch eine Meldung von Verstößen, deren Kenntnis ein Datenschutzbeauftragter außerhalb seiner Überprüfungsaufgabe erlangte, an die Aufsichtsbehörden ist von der Pflicht zur Zusammenarbeit nicht umfasst. Dies resultiert direkt aus der in Art. 38 Abs. 5 DS-GVO enthaltenen Pflicht zur Wahrung der Geheimhaltung oder der Vertraulichkeit[12]. Es gilt gleichermaßen auch für die Pflichten, welche aus der EU-Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen[13] (Geschäftsgeheimnisse) beziehungsweise deren Umsetzung ins deutsche Recht, dem Gesetz zum Schutz von Geschäftsgeheimnissen[14] (GeschGehG) resultieren. Entsprechend § 4 Abs. 2 Ziff. 3 GeschGehG darf ein Geschäftsgeheimnis nicht offengelegt werden, wenn dabei gegen eine Verpflichtung das Geschäftsgeheimnis nicht offenzulegen, wie es Art. 38 Abs. 5 DS-GVO darstellt, verstoßen wird.

Personenbezogene Daten erfüllen häufig die in § 2 Abs. 1 Nr. 1 GeschGehG enthaltenen Kriterien eines Geschäftsgeheimnisses[15]. Damit können insbesondere auch Verstöße gegen Datenschutzrecht ein Geschäftsgeheimnis i. S. d § 2 Ziff. 1 GeschGehG darstellen.

[7] Artikel-29-Datenschutzgruppe: Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), Abschnitt „Anhang zu den DSB-Leitlinien: Was sie wissen müssen", Ziffer 10. Zuletzt überarbeitet und angenommen am 5. April 2017, vom Europäischen Datenschutzausschuss bestätigt am 25. May 2018. Online, zitiert am 2022-01-18; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_de

[8] BAG, Urt. v. 24. Mai 2018, Az. 2 AZR 72/18, Rn. 25. Online, zitiert am 2022-01-18; verfügbar unter https://dejure.org/2018,13188 bzw. Volltext unter https://www.bag-urteil.com/24-05-2018-2-azr-72-18/

[9] BAG, Urt. v. 9 Juni 2011, AZ. 6 AZR 687/09, Rn. 14. Online, zitiert am 2022-01-18; verfügbar unter https://dejure.org/2011,167 bzw. Volltext unter https://www.bag-urteil.com/09-06-2011-bag-6-azr-68709/#14

[10] BAG, Urt. v. 9 Juni 2011, AZ. 6 AZR 687/09, Rn. 18. BAG, Urt. v. 24. Mai 2018, Az. 2 AZR 72/18, Rn. 25.

[11] So z. B.

- Drewers S.: Art. 39 Rn. 36. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7

- Bergt M.: Art. 39 Rn. 19. In: Kühling/Buchner (Hrsg.) DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0

[12] Paal BP.: Art. 39 Rn. 8 In: Paal/Pauly (Hrsg.) Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG. C. H. Beck Verlag, 3. Auflage 2021. ISBN: 978-3-406-75374-9

[13] Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Online, zitiert am 2022-01-18; verfügbar unter https://eur-lex.europa.eu/eli/dir/2016/943/oj?locale=de#:~:text=Directive%20%28EU%29%202016%2F943%20of%20the%20European%20Parliament%20and,acquisition%2C%20use%20and%20disclosure%20%28Text%20with%20EEA%20relevance%29

[14] Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG). Online, zitiert am 2022-01-18; verfügbar unter https://www.gesetze-im-internet.de/geschgehg/index.html#BJNR046610019BJNE000300000

[15] Gola P. (2020) Der betriebliche Datenschutzbeauftragte als „Geheimnisträger". PinG: 87

Der Datenschutzbeauftragte muss – werden ihm Datenschutzverstöße bekannt – entsprechend Art. 39 Abs. 1 lit. a DS-GVO unverzüglich den Verantwortlichen informieren und diesen hinsichtlich einer Beseitigung der Verstöße[16] und seiner damit im Zusammenhang stehenden datenschutzrechtlichen Pflichten beraten. Bei der Suche nach einer Lösung, wie die Datenschutzverstöße abgestellt werden können, kann sich ein Datenschutzbeauftragter gegebenenfalls gemäß Art. 39 Abs. 1 lit. e DS-GVO an die zuständige Aufsichtsbehörde wenden, wenn hierdurch die Treuepflicht nicht verletzt wird. Die Treuepflicht wie auch die Pflicht zur vertrauensvollen Zusammenarbeit gegenüber dem Arbeit- oder Auftraggeber erfordert im Regelfall, dass bei einer Verarbeitung personenbezogener Daten, die nicht im Einklang mit den datenschutzrechtlichen Vorschriften steht, zunächst alle internen Möglichkeiten zur Abhilfe genutzt werden.[16]

Bleibt es trotz Information der höchsten Managementebene und der Darstellung möglicher Abhilfemaßnahmen durch den Datenschutzbeauftragten bei Zuwiderhandlungen gegen die DS-GVO oder andere Datenschutzvorschriften oder beinhaltet die Verarbeitung eine schwere Beeinträchtigung für die Rechte und Freiheiten betroffener Personen, so wird vereinzelt in der Literatur auch die Auffassung vertreten, dass der Datenschutzbeauftragte verpflichtet ist, die Aufsichtsbehörde zu informieren.[17] An anderer Stelle wird von einer Meldepflicht nur bei schwersten Verstößen, insbesondere bei Straftaten, ausgegangen.[11,18]

„Beratung zu allen sonstigen Fragen"

In der englischen Fassung von Art. 39 Abs. 1 lit. e DS-GVO steht „and to consult, where appropriate, with regard to any other matter", in der deutschen Fassung mit „und gegebenenfalls Beratung zu allen sonstigen Fragen" übersetzt. Dieser Passus betrifft, wie es in der englischen Fassung deutlicher betont wird, die Aufgabe der Aufsichtsbehörden den Datenschutzbeauftragten zu beraten.[19] Gemäß Art. 57 Abs. 3 DS-GVO kann der Datenschutzbeauftragte diese Beratungsaufgabe der Aufsichtsbehörden kostenlos in Anspruch nehmen[20] – aber natürlich muss er dies nicht tun.[21]

Fazit:

Die Zusammenarbeit der Datenschutzbeauftragten mit den Aufsichtsbehörden und ihre Tätigkeit als Anlaufstelle für Aufsichtsbehörden sind in der DS-GVO nicht detailliert und ausdrücklich geregelt. Dies darf in der Praxis allerdings nicht dazu führen, dass durch zu weite Auslegung dieser Aufgaben eine Verlagerung der innerbetrieblichen Kontrollfunktion der Datenschutzbeauftragten hin zu einer Funktion als „verlängerter Arm" der Aufsichtsbehörden erfolgt. Vor allem darf die Zusammenarbeit nicht die Position und das Verhältnis der Datenschutzbeauftragten zu ihren Arbeit- oder Auftraggebern schwächen und für sie zu erhöhten Haftungs- oder anderen juristischen Risiken führen.

Über die Autoren

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

Dr. Bernd Schütze
beschäftigt sich seit 1995 mit den datenschutzrechtlichen Aspekten innerhalb der Gesundheitsversorgung. Nach gut dreißigjähriger beruflicher Tätigkeit in verschiedenen Krankenhäusern arbeitet Dr. Schütze seit 2014 als „Senior Experte Medical Data Security" bei der Deutschen Telekom Healthcare and Security Solutions GmbH. Als Lehrbeauftragter ist er zudem an verschiedenen Hochschulen tätig und veröffentlicht regelmäßig Beiträge in Büchern und Fachzeitschriften.

[16] Heberlein H.: Art. 39 Rn. 19. In: Ehmann/Selmayr (Hrsg.) Datenschutz-Grundverordnung. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-72006-2

[17] Bergt M.: Art. 39 Rn. 19. In: Kühling/Buchner (Hrsg.) DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0

[18] Bergt M.: Art. 39 Rn. 19. In: Kühling/Buchner (Hrsg.) DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-

[19] So z. B.

- Drewers S.: Art. 39 Rn. 37. In: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3-8487-3590-7
- Kahlert F, Licht S. (2016) Die neue Rolle des Datenschutzbeauftragten nach der DSGVO – Was Unternehmen zu beachten haben. ITRB: 181
- Bergt M.: Art. 39 Rn. 20. In: Kühling/Buchner (Hrsg.) DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0
- Heberlein H.: Art 39 Rn. 19. In: Ehmann/Selmayr (Hrsg.) Datenschutz-Grundverordnung. C. H. Beck Verlag, 2. Auflage 2018. ISBN 978-3-406-72006-2
- Artikel-29-Datenschutzgruppe: Leitlinien in Bezug auf Datenschutzbeauftragte („DSB"), Abschnitt 4.3. Zuletzt überarbeitet und angenommen am 5. April 2017, vom Europäischen Datenschutzausschuss bestätigt am 25. May 2018. Online, zitiert am 2022-01-18; verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-officer_de

[20] Raum B.: Art. 39 Rn. 39. In: Eßer/Kramer/ von Lewinski (Hrsg.) Auernhammer, DSGVO / BDSG – Kommentar. Carl Heymanns Verlag, 7. Auflage 2020. ISBN 978-3-452-29526-2

[21] Bergt M.: Art. 39 Rn. 20. In: Kühling/Buchner (Hrsg.) DS-GVO Bundesdatenschutzgesetz Kommentar. C. H. Beck Verlag, 3. Auflage 2020. ISBN 978-3-406-74994-0

WIRD DER DATENSCHUTZ ZUKÜNFTIG DURCH PRIVATE DURCHGESETZT?

Landgericht Saarbrücken legt dem EuGH vier Fragen zu Art. 82 DS-GVO vor

Stefan Sander, LL.M., B.Sc.

Die Durchsetzung des Datenschutzrechts ist Aufgabe der Aufsichtsbehörden („public law enforcement"), jedenfalls nach Ansicht des europäischen Gesetzgebers. Die deutschen Aufsichtsbehörden vertreten indes eine andere Ansicht und verstehen ihren Job vielfach dahin, auf die Einhaltung des Datenschutzrechts hinzuwirken, indem sie Unternehmen wie Behörden beraten anstatt bestrafen. Eine effektive Sanktionierung ist so flächendeckend kaum möglich. Die deutschen Gesetzgeber steuern zudem ihre Teile dazu bei (vgl. § 43 Abs. 3 BDSG und Entsprechungen in den Landesgesetzen). Diese „weichgespülte" Herangehensweise führt dazu, dass Verfolgungsdruck fehlt – und Datenschutzverstöße in Unternehmen wie Behörden System haben. Immer wieder bauen Verantwortliche ganze Geschäftsmodelle auf rechtswidrigen Verarbeitungen auf, denn das Risiko tatsächlich durch die Aufsichtsbehörden von diesem (profitablen) Handeln abgebracht zu werden, konvergiert gegen Null. Das Blatt könnte sich jedoch bald wenden: Der EuGH hat es in der Hand zu entscheiden, ob die betroffene Person selbst als Kontrollinstanz neben die Aufsichtsbehörden tritt. Er wird zu entscheiden haben, ob und wenn ja mit welchen Mitteln (z.B. sog. „Strafschadensersatz") zukünftig eine private Rechtsdurchsetzung („private law enforcement") der rechtswidrigen Verarbeitung personenbezogener Daten Einhalt gebietet.

I. Sachverhalt

Der Entscheidung des LG Saarbrücken (Beschl. v. 22.11.2021 – 5 O 151/19)[1] liegen folgende tatsächliche Umstände zugrunde:

Nachdem die beklagte Gesellschaft im Rahmen einer Auskunft gem. Art. 15 DS-GVO mitgeteilt hatte Daten in Bezug auf den Kläger auch zu Werbezwecken zu verarbeiten, widerrief dieser vorsorglich alle etwaig von ihm erteilten Einwilligungen und widersprach Verarbeitungen zum Zwecke von Direktwerbung. Rund drei Monate danach versandte die Beklagte an den Kläger postalisch zwei persönlich adressierte Werbeschreiben, jeweils versehen mit individueller Anrede. Der Kläger widersprach ein zweites Mal Verarbeitungen zum Zwecke von Direktwerbung. Wiederum drei Wochen später versandte die Beklagte an den Kläger erneut per Post ein weiteres persönlich adressiertes Werbeschreiben, ebenfalls versehen mit individueller Anrede. Der Kläger widersprach ein drittes Mal Verarbeitungen zum Zwecke von Direktwerbung.

Jedes dieser drei Werbeschreiben enthielt einen personalisierten Rabattcoupon und die Aufforderung, diesen im Webshop der Beklagten einzulösen. Ca. drei Wochen nach dem dritten Widerspruchsschreiben suchte der Kläger den Webshop der Beklagten auf und fand dort eine marktübliche Bestellmaske vor. Neben den Feldern zur Eingabe von Namen und Adresse sowie weiteren Angaben zu Person, die erwartungsgemäß beim Seitenaufruf alle leer waren, fand sich auch ein Feld zur Eingabe von Rabattcoupons. Der Kläger gab sodann dort den Rabattcoupon des letzten an ihn adressierten Werbeschreibens ein, woraufhin sich die Bestellmaske mit Angaben zu seiner Person füllte, so dass zwecks Abschlusses der Bestellung nur noch ein Produkt der Beklagten auszuwählen gewesen wäre.

Die Beklagte hat einen Prozess zur Bearbeitung von Werbewidersprüchen implementiert. Dass nach dem ersten Widerspruch dennoch Werbebriefe versandt wurden, beruhte darauf, dass ein

[1] Offenlegung: Der Autor ist klägerseitig am Verfahren beteiligt.

einzelner Mitarbeiter sich weisungswidrig verhielt. Der Versand des Werbeschreibens nach dem zweiten Widerspruch beruhte darauf, dass der Widerspruch, nachdem das Schreiben bereits in Auftrag gegeben war, nur mit – nach Ansicht der Beklagten: unverhältnismäßig hohem – Aufwand hätte umgesetzt werden können.

II. Vorlagefragen an den EuGH

Das Vorabentscheidungsersuchen des LG Saarbrücken wird beim EuGH als Rs. C-741/21 geführt. Das Gericht formulierte diese vier Fragen an den EuGH:

1. Ist der Begriff des immateriellen Schadens in Art. 82 Abs. 1 DS-GVO im Hinblick auf den Erwägungsgrund 85 und den Erwägungsgrund 146 S. 3 DS-GVO in dem Sinne zu verstehen, dass er jede Beeinträchtigung der geschützten Rechtsposition erfasst, unabhängig von deren sonstigen Auswirkungen und deren Erheblichkeit?

2. Wird die Haftung auf Schadenersatz gemäß Art. 82 Abs. 3 DS-GVO dadurch ausgeschlossen, dass der Rechtsverstoß auf menschliches Versagen im Einzelfall einer im Sinne von Art. 29 DS-GVO unterstellten Person zurückgeführt wird?

3. Ist bei der Bemessung des immateriellen Schadenersatzes eine Orientierung an den in Art. 83 DS-GVO, insbesondere Art. 83 Abs. 2 und Abs. 5 DS-GVO genannten Zumessungskriterien erlaubt bzw. geboten?

4. Ist der Schadenersatz für jeden einzelnen Verstoß zu bestimmen oder werden mehrere – zumindest mehrere gleichgelagerte – Verstöße mit einer Gesamtentschädigung sanktioniert, die nicht durch eine Addition von Einzelbeträgen ermittelt wird, sondern auf einer wertenden Gesamtbetrachtung beruht?

III. Kontext der Fragestellungen

1. Frage: Schaden und Rechtsgutverletzung

Der Kläger stützt seinen Anspruch auf den Umstand, dass seine Daten ohne Berücksichtigung seines Widerspruchs für Zwecke der Direktwerbung verarbeitet (insb. „gespeichert", zur Herstellung von Druckerzeugnissen „verwendet" sowie zur Vorbefüllung der Bestellmaske „ausgelesen") wurden. Rechtsfragen rund um die u.a. für das Dialogmarketing wichtige Einwilligung[2] waren nicht relevant. Da die Beklagte im Rahmen von Art. 21 Abs. 2 DS-GVO, anders als bei Widersprüchen gem. Art. 21 Abs. 1 DS-GVO keinerlei Möglichkeiten hat den Widerspruch als unbegründet zurückzuweisen oder ihn mittels „zwingender schutzwürdiger Gründe für die Verarbeitung" zu übersteuern, ordnet Art. 21 Abs. 3 DS-GVO folgerichtig an, dass der Verantwortliche die Verarbeitung für Zwecke der Direktwerbung zu unterlassen hat. Ab wann solche Verarbeitungen zu unterbleiben haben, ist dort nicht näher ausformuliert. Die gesetzlichen Vorgaben, welche die zeitlich den vorgenannten Verarbeitungen (insb. Speichern, Verwenden, Auslesen) nachfolgende „werbliche Ansprache" in Abhängigkeit des Kommunikationsmittels regeln (Art. 95 DS-GVO i.V.m. Art. 13 Richtlinie 2002/58/EG i.V.m. § 7 UWG), waren nicht relevant.

Es ist allein der Verstoß gegen das „Verbot mit Erlaubnisvorbehalt", mithin die materiell rechtswidrige Verarbeitung der personenbezogenen Daten, der nach dem Vortrag des Klägers die Grundlage des Schadensersatzanspruchs gem. Art. 82 DS-GVO sein soll – die Verletzung anderer Rechtsgüter wurde nicht vorgetragen. Dabei gibt der einleitende Halbsatz von Art. 6 Abs. 1 DS-GVO („ist nur rechtmäßig, wenn") lediglich sinngemäß die Formulierung wieder, die in Art. 8 Abs. 2 der europäischen Grundrechtecharta (GRCh) gewählt wurde („dürfen nur [wenn]"). Verletzt wurde demnach das Grundrecht auf Schutz personenbezogener Daten.

Vor diesem Hintergrund stellt sich die Frage, ob bereits ein Verstoß gegen die DS-GVO einen Schaden i.S.v. Art. 82 DS-GVO begründen kann, ohne dass weitere Rechtspositionen beeinträchtigt werden (sonstige Auswirkungen wie z.B. Verletzungen der Gesundheit („emotional distress") oder Belästigungen[3]). Dies könnte der Fall sein, wenn die verletzte Vorschrift der DS-GVO ein subjektives Recht

[2] EuGH, Urt. v. 1.10.2019 – C-673/17; EuGH, Urt. v. 11.11.2020 – C-61/19.

[3] Zu Art. 13 Richtlinie 2002/58/EG, der durch § 7 UWG umgesetzt wird, entschied der EuGH (Urt. v. 25.11.2021 – C-102/20), dass die Richtlinie nicht das Erfordernis vorschreibt festzustellen, dass die Belastung des Nutzers über eine Belästigung hinausgeht. Zugleich stellt der Gerichtshof fest, dass eine solche Einblendung von Werbenachrichten dem Nutzer jedenfalls tatsächlich eine Belastung auferlegt.

der betroffenen Person betrifft beziehungsweise ihr ein solches gewährt.[4] Neben den materiell rechtswidrigen Verarbeitungen, also Verarbeitungen, die gegen das Verbot mit Erlaubnisvorbehalt verstoßen (Kapitel II der DS-GVO), kommen daher jedenfalls auch Verstöße gegen die Rechte der betroffenen Person (Kapitel III der DS-GVO) in Betracht. Keinen Schaden i.S.v. Art. 82 DS-GVO stellen hingegen Verstöße gegen objektive Rechtspflichten dar, beispielsweise solche zur Dokumentation gem. Art. 30 DS-GVO.

Die Frage nach der Erheblichkeitsschwelle ist hingegen nicht mehr als die Aufarbeitung beziehungsweise Bewältigung deutscher Rechtshistorie. Auch Bagatellen führen bei Vorliegen der Tatbestandsmerkmale gem. Art. 82 Abs. 1 DS-GVO dem Grunde nach zu Ansprüchen (anders als i.R.v. § 8 Abs. 2 BDSG a.F., der nur bei „schweren Verletzungen des Persönlichkeitsrechts" dem Grunde nach Ansprüche gewährte), lediglich der Höhe nach sind diese i.R.v. Art. 82 DS-GVO angemessen zu behandeln. Die mannigfachen Verarbeitungen i.S.v. Art. 4 Nr. 2 DS-GVO im vorliegendem Fall, die gegen den in der GRCh niedergeschriebenen Kern des Datenschutzrechts, mithin das Verbot mit Erlaubnisvorbehalt verstießen, können unter keinem denkbaren Blickwinkel als Bagatellen bewertet werden. Wie eine angemessene Behandlung erfolgen kann, soll Frage 3 klären.

2. Frage: Verschulden im Rahmen der Haftungsbegründung und -befreiung

Das Landgericht Saarbrücken sieht in Art. 82 DS-GVO eine Haftung für vermutetes Verschulden und sieht sich mit der Frage konfrontiert, ob das menschliche Versagen eines Mitarbeiters (Fahrlässigkeit) dazu führt, dass der Arbeitgeber im Außenverhältnis von der Haftung frei wird. Die DS-GVO ist jedoch hinsichtlich der „unterstellten Personen" sehr sparsam mit Regelungen und so findet sich weder eine Zurechnungsnorm entsprechend § 278 S. 1 BGB noch eine Haftung für vermutetes, eigenes Verschulden entsprechend § 831 Abs. 1 BGB. Stattdessen regelt Art. 82 Abs. 3 DS-GVO die Rechtsfolge, die an das Vorliegen eines Nachweises geknüpft ist. Welche konkreten Anforderungen an diesen Nachweis zu stellen sind, ergibt sich aus der Vorschrift nicht, insbesondere bleibt offen, ob „verantwortlich" im Sinne von vorsätzlich oder fahrlässig zu verstehen ist und welche Bedeutung der Formulierung „in keinerlei Hinsicht" zukommt.

Da der EuGH bereits entschieden hat[5], dass der Begriff des Verschuldens in den verschiedenen Rechtsordnungen der Gemeinschaft nicht den gleichen Inhalt hat, wird der Begriff „Verschulden" in der Diskussion um den Anspruch aus Art. 82 DS-GVO wohl zu vermeiden sein. Demnach wird Art. 82 Abs. 1 DS-GVO als eine verschuldensunabhängige Haftung zu sehen sein, die einer rechtsvernichtenden Einwendung gem. Art. 82 Abs. 3 DS-GVO begegnet. Dies hätte zur Folge, dass an den Tatbestand der Einwendung strengere Anforderungen gestellt werden könnten als an die Widerlegung der Vermutung eines Verschuldens. Vor dem Hintergrund der Rechtsprechung des EuGH zur gemeinsamen Verantwortlichkeit in Sachen „Zeugen Jehovas"[6] dürfte es wahrscheinlich sein, dass der EuGH strenge Anforderungen an die rechtsvernichtende Einwendung stellt. Dort war aufgrund von geringen inhaltlichen Anforderungen das Vorliegen einer „gemeinsamen Entscheidung" (vgl. Art. 4 Nr. 7 DS-GVO) angenommen worden, was zur Vermeidung von Wertungswidersprüchen bei der Frage zu berücksichtigen ist, wann ein Rechtsträger „in keinerlei Hinsicht" verantwortlich bzw. haftbar ist (vgl. Art. 82 Abs. 3 DS-GVO).

3. Frage: Anwendbares Recht zur Bestimmung der Rechtsfolge

Ob Art. 82 DS-GVO nicht nur die Anspruchsgrundlage, sondern auch die Rechtsfolge regelt, ist offen. In ähnlichen Konstellationen ist nach Ansicht des EuGH das nationale Recht zur Ergänzung des europäischen Rechts überall dort heranzuziehen, wo das europäische Recht ergänzungsbedürftig ist. Vor diesem Hintergrund dürften in Deutschland die §§ 249 ff. BGB auf Rechtsfolgenseite zur Anwendung kommen.[7]
Maßgeblich zu beachten sein wird jedoch, dass das sodann angewendete nationale Recht im Lichte des europäischen Rechts auszulegen ist, zu dessen Ergänzung es herangezogen wird. Denn es folgt aus den Anforderungen sowohl der einheitlichen Anwendung des Unionsrechts als auch des Gleichheitsgrundsatzes, dass die Begriffe einer Vorschrift des Unionsrechts, die für die Ermittlung ihres Sinnes und ihrer Tragweite nicht ausdrücklich auf das Recht der Mitglied-

[4] Diese Argumentation nimmt Bezug auf die Urteile des EuGH C 98/14, Rn. 104, C 46/93 und C 48/93, Rn. 51, C 445/06, Rn. 20 und C 379/10, Rn. 40.

[5] EuGH, Urt. v. 05.03.1996 - C-46/93, C-48/93 (Rn. 83).

[6] EuGH, Urt. v. 10.07.2018 – C-25/17.

[7] Argumentation entsprechend EuGH, Urt. v. 05.03.1996 - C-46/93, C-48/9, wiederholt bestätigt, zuletzt etwa durch EuGH, Urt. 14.09.2017 - C 628/15.

Der Europäische Gerichtshof (EUgH) in Luxemburg (Foto: G. Fessy/CJUE).

staaten verweist, in der Regel in der gesamten Union eine autonome und einheitliche Auslegung erhalten müssen.[8] Während in Deutschland Anspruchsgrundlagen, die Schadensersatz gewähren, allein die Funktion der „Kompensation" aufweisen, ist dies im europäischen Recht mit Blick auf die weitere Funktion „Verhaltenssteuerung"[9] anders: Der EuGH bezeichnet Schadensersatzklagen wegen Verstößen gegen die Wettbewerbsregeln als „einen integralen Bestandteil des Systems zur Durchsetzung dieser Vorschriften, das darauf abzielt, wettbewerbswidriges Verhalten der Unternehmen zu ahnden und diese von der Beteiligung an solchem Verhalten abzuhalten". [10] Auch hat der EuGH bereits mehrfach ausgeführt, dass der Ausgleich von Schäden „auf eine abschreckende und angemessene Art und Weise geschehen" müsse.[11] Entschädigungen müssen, „damit ihre Wirksamkeit und ihre abschreckende Wirkung gewährleistet sind, in einem angemessenen Verhältnis zu dem erlittenen Schaden stehen"[12], wobei letzteres den vollumfänglichen Ausgleich der tatsächlich entstandenen Schäden meint.[13] Dies steht einer Beschränkung auf rein symbolische Entschädigungen[14] sowie der Festlegung von Obergrenzen[15] entgegen.

Zwar hat Art. 83 DS-GVO die Verhängung von Geldbußen zum Gegenstand, doch erscheinen nach Ansicht des hier erkennenden Gerichts die dort aufgezeigten Zumessungskriterien auch für die Bemessung von Geldentschädigungen für immaterielle Schäden geeignet und effektiv. Zudem würde durch die einheitliche Anwendung dieser Kriterien in allen Mitgliedstaaten dem Gebot des wirksamen Schadenersatzes (Erwägungsgrund 146) Rechnung getragen. Die Vorlagefrage ist hier von besonderer Bedeutung, weil in Art. 83 Abs. 5 DS-GVO für bestimmte Verstöße (unter anderem gegen Art. 6 und Art. 21 DS-GVO) im Falle eines Unternehmens der Jahresumsatz als Bemessungsgröße vorgegeben ist. Konkreten Sachvortrag zum Jahresumsatz der Beklagten ermöglichten die Veröffentlichungen im Handelsregister.

4. Frage: Umfang eines immateriellen Schadens bzw. Rechtsfolge

Das LG Saarbrücken stellte sich die Frage, ob jeder einzelne Verstoß der Beklagten gegen die DS-GVO isoliert zu behandeln und einzeln zu sanktionieren ist oder ob – zumindest für mehrere gleichgelagerte Verstöße – eine Gesamtentschädigung zu bestimmen ist. Daran schließt sich die Frage an, ob für die zu bildende

[8] EuGH, Urt. v. 1.10.2019 – C 673/17, Rn. 47.
[9] Vgl. dazu auch Vorlage des BAG, Beschl. v. 26.08.2021 – 8 AZR 253/20 (A): Hat Art. 82 Abs. 1 DSGVO spezial- bzw. generalpräventiven Charakter?
[10] St. Rspr., zuletzt EuGH, Urt. v. 14.03.2019 - C-724/17 (zum Kartellschadensersatzrecht).
[11] EuGH, Urt. v. 17.12.2015 – C-407/14 (m. w. N.).
[12] EuGH, Urt. v. 10.04.1984 – 14/83.
[13] EuGH, Urt. v. 02.08.1993 – C-271/91
[14] EuGH, Urt. v. 10.04.1984 – 14/83.
[15] EuGH, Urt. v. 02.08.1993 – C 271/91.

Gesamtentschädigung Einzelbeträge für jeden Verstoß auszuwerfen sind, die dann in einen Gesamtbetrag – aber nicht durch Addition der Einzelbeträge – Eingang finden oder ob eine Gesamtentschädigung auf der Grundlage einer wertenden Gesamtbetrachtung ermittelt werden soll.

Durch die drei Widersprüche i.S.v. Art. 21 Abs. 2 DS-GVO wurde ein ansonsten zusammenhängendes Geschehen jeweils unterbrochen. Als ein solches Geschehen könnte die Verarbeitungstätigkeit im Sinne von Art. 30 Abs. 1 DS-GVO gesehen werden, welche aus den diversen Verarbeitungen im Sinne von Art. 4 Nr. 2 DS-GVO bestand, die die Beklagte zum Zwecke der Direktwerbung ausführte. Fraglich ist die Auslegung von Art. 82 Abs. 1 DS-GVO, der „wegen eines Verstoßes" einen Anspruch auf Schadenersatz gewährt: Wird auf die zahlreichen einzelnen Verarbeitungen abzustellen sein und falls ja wie ist die fortgesetzte Speicherung zu bewerten? Oder handelt es sich womöglich um eine rechtswidrige Verarbeitung pro Tag? Ist es der Verstoß gegen Art. 6 Abs. 1 DS-GVO oder jener gegen Art. 21 Abs. 3 DS-GVO? Sollte ggf. vorzugswürdiger anstatt auf die rechtswidrigen Verarbeitungen auf das Unterlassen der Umsetzung eines Widerspruchs Bezug genommen werden, als der Verletzung eines Rechts der betroffenen Person? Und falls ja, sind es drei einzeln zu beurteilende Verstöße oder können sie zusammenfassend betrachtet werden?

Fragen zur Auslegung des Wortlautes „wegen eines Verstoßes" sind dabei nicht neu (vgl. z.B. strafbewehrte Unterlassungserklärungen), sondern werden in Deutschland seit Langem durch die Grundsätze der sog. „natürlichen Handlungseinheit" beantwortet. Sie finden auch Anwendung bei der Vollstreckung eines zivilgerichtlichen Urteils, mit dem der Schuldner zur Unterlassung verurteilt wurde und ihm zugleich „für jeden Fall" der Zuwiderhandlung gegen das Urteil die Festsetzung eines Ordnungsmittels gem. § 890 ZPO angedroht wurde.[16] Diese Grundsätze könnten einen sachgerechten Lösungsvorschlag für diese Vorlagefrage darstellen.

[16] BGH, Beschl. v. 17.12.2020 – I ZB 99/19.

Überweisungen an den EuGH

Kommt es in einem deutschen Rechtsstreit auf die Auslegung einer europäischen Verordnung oder Richtlinie an, kann oder muss der EuGH eingebunden werden. Dazu wird in der Regel der anhängige Rechtsstreit der Parteien „pausiert", indem das Verfahren durch Beschluss analog § 148 ZPO ausgesetzt wird. Das Gericht leitet sodann von sich aus ein neues Verfahren ein, indem es in eigenem Namen ein Ersuchen um Vorabentscheidung an den EuGH richtet. Die Parteien des Ausgangsrechtsstreits haben im Vorabentscheidungsverfahren vor dem EuGH als Beteiligte die Möglichkeit, sich zu den Rechtsfragen zu äußern. Alle Gerichte aller Mitgliedsstaaten sind berechtigt, Ersuchen um Vorabentscheidungen auf der Grundlage von Art. 267 AEUV an den EuGH zu richten – letztinstanzliche Gerichte müssen es, wenn die Entscheidung des Rechtsstreits von der Auslegung des EU-Rechts abhängt.

Über den Autor

Stefan Sander LL.M., B.Sc.

ist Rechtsanwalt und Fachanwalt für IT-Recht, zudem Software-Systemingenieur und Datenschutzbeauftragter (TÜV). Er führt mit Heiko Schöning die Kanzlei sds Rechtsanwälte Sander Schöning PartG mbH.

▶ www.sds.ruhr

sds Rechtsanwälte Sander Schöning PartG mbB

Anzeige

Jetzt bestellen und im Bereich Datenschutz auf dem neuesten Stand sein!

- seit über 40 Jahren
- monatlich
- topaktuell informiert über die wichtigsten Neuigkeiten, Risiken und die aktuelle Rechtsprechung
- mit konkreten Handlungsempfehlungen, Arbeitsmitteln und Checklisten für die tägliche Praxis

www.datenschutz-berater.de

- Seit über 40 Jahren ist der monatlich erscheinende **DATENSCHUTZ-BERATER** der verlässliche Ratgeber für Datenschutz und Datensicherheit. Mit den täglich wachsenden Möglichkeiten der Datenerhebung, -verarbeitung und -nutzung wird Datenschutz immer wichtiger. Technische und rechtliche Neuerungen, Risiken und die aktuelle Rechtsprechung fordern von den Verantwortlichen, sich fortlaufend zu informieren. Der Fachleser profitiert von konkreten Handlungsempfehlungen, Arbeitsmitteln und Checklisten für die tägliche Praxis. Literaturtipps und Terminhinweise für Aus- und Weiterbildung runden das Angebot ab.
- Zielgruppe sind Fach- und Führungskräfte der Datenschutzabteilung, Personalabteilung, interne und externe Datenschutzbeauftragte, Datenschutzabteilungen, Geschäftsführer, IT-Sicherheitsexperten und Revisoren.
- Die **R&W-Online Datenbank** online.ruw.de – mit allen Inhalten der R&W-Zeitschriften und des R&W-Buchportfolios – bietet eine publikationsübergreifende, schnelle und zuverlässige Recherchemöglichkeit. Highlights sind die Übersichtlichkeit, Bedienerfreundlichkeit und besonders die pdf-Darstellung gemäß des Original-Seitenlayouts.

Per Faxantwort an 069/7595-1150

Name: _____

Firma: _____

Abteilung: _____

Straße: _____

PLZ | Ort: _____

Telefon: _____

E-Mail: _____

Datum | Unterschrift: _____

Sichern Sie sich Ihr individuelles Vorteilsangebot und bestellen Sie jetzt den DSB – Datenschutz-Berater

☐ **Testabo:** 3 Monate kostenlos lesen + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 3 Ausgaben der Fachzeitschrift „Datenschutz-Berater" kostenlos. Falls Ihnen der „Datenschutz-Berater" gefällt, brauchen Sie nichts weiter zu unternehmen. Wenn Sie nicht innerhalb der Testzeit abbestellen, beginnt im Anschluss ein Jahresabo. Zunächst für ein Jahr (11 Ausgaben) zum Vorzugspreis von derzeit 359,- € inkl. aller Gebühren und MwSt. in Deutschland und anschließend bis auf Widerruf zum jeweils gültigen Jahrespreis. Das Abonnement kann bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar.

☐ **Jahresabo:** 11 Ausgaben + 1 Zugang zur Online-Datenbank

Sie erhalten die nächsten 11 Ausgaben der Fachzeitschrift „Datenschutz-Berater", sowie den Zugang zur Online-Datenbank. Der Abonnementvertrag wird für mindestens ein Jahr abgeschlossen. Das Abonnement kann jederzeit bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar und betragen 359,- € inkl. aller Gebühren und MwSt. in Deutschland.

DATENSCHUTZ-BERATER
kundenservice@ruw.de

dfv Mediengruppe

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!

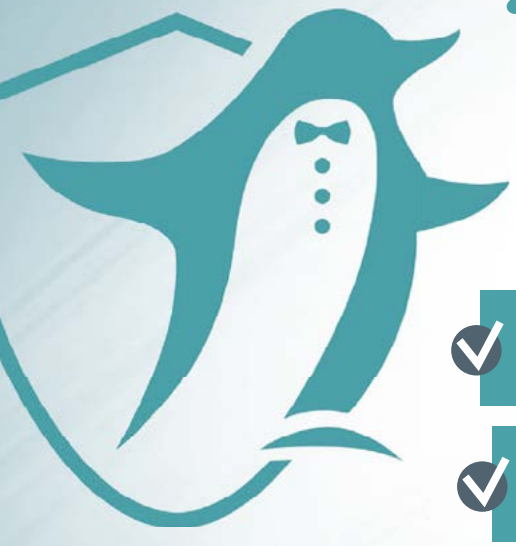
Ich führe deine Kunden mit intuitiven **Online-Fragebögen** durch die Ersterhebung und alle weiteren Datenschutzaudits. Damit deine Kunden wissen, was als nächstes zu tun ist, ordne ich ihnen auch automatisiert **Aufgaben und Datenschutzmaßnahmen** zu.

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 Tiefenscans 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

9 VON 10 WEBSEITEN NICHT RECHTSSICHER - STEHT AUCH IHR NAME ALS DATENSCHUTZBEAUFTRAGTER AUF EINER SOLCHEN SEITE?

Daniel Lukmann

Sie erstellen für Ihre Mandanten die Datenschutzerklärung? Sie sehen sich den Cookie Banner an und prüfen die Seite auch auf Datenschutz-Lücken? Ja? Aber sind Sie auch wirklich sicher, ob Sie tatsächlich alle Verstöße aufdecken konnten?

Fakt ist: 9 von 10 Webseiten sind trotz der Überprüfung eines Datenschutzbeauftragten (DSB) nicht rechtskonform! Und das jedoch nicht aufgrund von fehlendem Know-How, sondern weil es ohne technische Unterstützung und Tiefenscans nahezu unmöglich ist!

Blöd nur, wenn Ihr Name dann in der Datenschutzerklärung einer rechtswidrigen Webseite steht und Sie damit Ihren guten Ruf riskieren…

Was muss eigentlich geprüft werden?

Jeder Zugriff auf eine Webseite verursacht zwangsläufig den Austausch personenbezogener Daten, da seit dem EuGH-Urteil aus dem Jahr 2016 IP-Adressen als personenbezogen gelten. Die Gesetzgebung legt klare Regeln dafür fest, wie diese Daten auf Webseiten verarbeitet werden dürfen. So besteht u.a. die Pflicht zum Schutz von Besucherdaten. Daher müssen Sie als DSB z.B. regelmäßig prüfen, ob Cookies und externe Dienste ohne Einwilligung geladen werden oder ob es Datenübertragungen in unsichere Drittländer (z.B. USA) gibt. Zudem ist es wichtig, dass die Datenschutzerklärung immer aktuell gehalten wird – auch bei Änderungen auf der Webseite durch den Kunden.

Das Dilemma der Datenschutzbeauftragten

Als DSB haben Sie eine Hinweispflicht und müssen Ihre Kunden auch über Datenschutz-Lücken auf deren Webseiten informieren. Das Problem: Webseiten sind in erster Linie technische Konstrukte aus Programmzeilen und Quellcodes. Deshalb benötigen Sie also eigentlich eine in gleichen Maßen juristische, als auch technische Expertise. Und welcher DSB ist schon auch ein IT-Profi?

Prüfung aller Seiten und Quellcodes nahezu unmöglich

Problematisch ist auch der riesige Umfang der meisten Internetpräsenzen. Denn im Schnitt besteht EINE Webseite aus rund 200 Subseiten und Links, welche alle einzeln in Bezug auf den Datenschutz geprüft werden müssen. Und durch die umfangreichen Anforderungen der DSGVO ist es selbst für einen Datenschutz-Experten kaum noch möglich alle rechtlichen Erfordernisse auf einer Webseite zu erfüllen und diese laufend zu analysieren.

Schlechte Reputationen als Folge

Heutzutage sind Webseiten in der Regel dynamisch und es werden ständig Optimierungen vorgenommen, neue Plugins installiert oder Formulare hinzugefügt. Alles Punkte, bei denen man auch den Datenschutz berücksichtigen muss. Jedoch ist dies den meisten Betreibern von Webseiten gar nicht bewusst, weshalb Sie als DSB auch nicht darüber informiert werden. Folglich können Sie Ihren Kunden auch nicht darauf hinweisen, dass z.B. ein Eintrag in der Datenschutzerklärung hinzugefügt werden oder das Consent Tool neu konfiguriert werden muss. Und schon steht Ihr Name als DSB auf einer rechtswidrigen Webseite! Riskieren Sie also lieber keinen schlechten Ruf und überprüfen Sie regelmäßig den Online Auftritt Ihrer Kunden. Denn dieser ist auch das Aushängeschild für Ihre Arbeit als Datenschützer!

Tiefenscans und kontinuierlich Überwachung als Lösung

Um sicherzustellen, dass die Webseite immer den aktuellen rechtlichen Bestimmungen entspricht, sind Tiefenscans aller einzelnen Seiten und ein laufendes Monitoring essenziell. Dies ist allerdings nur mit einer entsprechenden technischen Unterstützung möglich – wie dem digitalen DSGVO Webseiten Butler ALFRIGHT.

Er scannt Webseiten inklusive ALLER Subseiten regelmäßig auf die Einhaltung rechtlicher Bestimmungen wie DSGVO, BDSG, EU-Cookie Richtlinie oder TTDSG. Zudem erstellt er auch eine passende Datenschutzerklärung und aktualisiert diese bei jedem neuen Scan. Dadurch ist ALFRIGHT die optimale Unterstützung für Betreiber großer Webseiten und externe Datenschutzbeauftragte.

Über den Autor

Daniel Lukmann
ist zertifizierter Datenschutzbeauftragter & CTO des digitalen DSGVO Webseiten Butlers ALFRIGHT.

▶ www.alfright.eu

ALFRIGHT
and your website fulfills all rights

ZERTIFIZIERUNG BRINGT MEHRWERT

Ziele und aktueller Stand des Zertifizierungsverfahrens nach der Datenschutz-Grundverordnung

Bettina Gayk, Henrike Postberg

Die Artikel 42 und 43 Datenschutz-Grundverordnung (DS-GVO) legen die Grundsteine für einheitliche europäische Zertifizierungs- und Akkreditierungsverfahren. Zertifikate sollen die Einhaltung der DS-GVO bei Verarbeitungsvorgängen einschließlich der Sicherheit der Verarbeitung nachweisen. Gleichzeitig dienen sie Marketing- und Geschäftszwecken. Bei einer Zertifizierung handelt es sich um einen objektiven Blick von außen, der auf möglicherweise eingefahrene Prozesse schaut und diese auf ihre Normgerechtigkeit prüft. Die externe Prüfung der eigenen Datenverarbeitungsprozesse verlangt denen, die zertifiziert werden möchten, ein hohes Maß an Strukturierung und intensiver Befassung mit den zu überprüfenden Prozessen ab.

Ein erteiltes Zertifikat hat mehrere Vorteile: Für alle, deren Daten verarbeitet werden, bedeutet es mehr Transparenz. Es ermöglicht betroffenen Personen einen raschen Überblick über das Datenschutzniveau von zertifizierten Produkten und Dienstleistungen.[1] Damit einhergehend wird die klare Botschaft formuliert, dass die zertifizierte Datenverarbeitung die Regeln der DS-GVO grundsätzlich einhält. Zertifizierung schafft also Vertrauen. Durch die regelmäßig stattfindenden Audits werden die Prozesse, die im Zertifikat benannt sind, überprüft und optimiert. Dies kann nicht nur potenzielle Kund*innen überzeugen, sondern auch Aufsichtsbehörden: Eine erfolgreiche Zertifizierung als solche garantiert zwar nicht die Einhaltung der DS-GVO bei jeder einzelnen Datenverarbeitung, sie attestiert aber, dass der zertifizierte Prozess grundsätzlich datenschutzkonform angelegt ist. Ein nach der DS-GVO erteiltes Zertifikat kann zudem bei aufsichtsbehördlichen Kontrollen von Vorteil sein und die Prüfung erleichtern. Im Einzelnen können die Zertifikate als Nachweis dienen, dass die folgenden Anforderungen erfüllt sind:

- Eine Zertifizierung kann für Verantwortliche als Gesichtspunkt herangezogen werden, um die Erfüllung ihrer Pflichten nachzuweisen (Art. 24 Abs. 3 DS-GVO).
- Dasselbe gilt für die Anforderungen beim Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 3 DS-GVO).
- Bei der Auftragsverarbeitung kommt einer Zertifizierung ebenfalls eine große Bedeutung zu: Ein Zertifikat kann als Nachweis dienen, dass ein Auftragsverarbeiter geeignete Garantien bietet (Art. 28 Abs. 5 DS-GVO), z. B. bei Cloud-Diensten, da deren Kunden und vor allem auch betroffene Personen sich selbst leichter ein Bild von einer bestimmten Verarbeitung hinsichtlich der Einhaltung der DS-GVO machen können. Auftragsverarbeiter können gegenüber Verantwortlichen nachweisen, dass sie zulässig ausgewählt werden dürfen und für die Qualität ihres Angebots werben. Verantwortliche können schnell erkennen, dass sich das Angebot für ihre Datenverarbeitung eignet.
- Eine Zertifizierung kann ferner als Faktor herangezogen werden, um die Sicherheit der Verarbeitung nachzuweisen (Art. 32 Abs. 3 DS-GVO).
- Außerdem können Zertifikate ein *Instrument für Datenübermittlungen* in unsichere Drittstaaten darstellen, wenn sie beispielsweise über Verträge rechtlich verbindlich gemacht werden (Art. 46 Abs. 2 Buchstabe f DS-GVO).

Zertifizierungen sind – wie Verhaltensregeln – in der DS-GVO als regulierte Selbstregulierung

[1] So auch Erwägungsgrund 100 der DS-GVO.

gestaltet. Das heißt, die Vorgaben werden nicht von den staatlichen Datenschutzaufsichtsbehörden gemacht und überwacht, sondern von anderen Akteuren[2]. Diese Vorgaben und die Überwachung werden von staatlichen Stellen genehmigt und kontrolliert. Die Aufgaben und Befugnisse der Datenschutzaufsichtsbehörden werden dadurch nicht eingeschränkt. Es treten vielmehr weitere Kontrollen hinzu. Das kann die Einhaltung von Datenschutzvorgaben und die Datenschutzaufsicht insgesamt verbessern und die Behörden entlasten.

Der folgende Überblick zeigt, was zertifiziert werden kann und wer zertifizieren darf. Ferner wird das Verfahren beschrieben, das Zertifizierungsstellen durchlaufen müssen, um als solche akkreditiert zu werden. Dieses komplexe und aufwendige Akkreditierungsverfahren soll die Qualität der Zertifizierungsstellen sichern und macht nachvollziehbar, warum es bisher noch keine DS-GVO-Zertifikate gibt. Schließlich folgt ein Ausblick auf den aktuellen Stand in Deutschland.

Was kann zertifiziert werden?

Gegenstand einer Zertifizierung können nur Datenverarbeitungen in Produkten, Verfahren oder Dienstleistungen von Verantwortlichen oder Auftragsverarbeitern sein.

Der Begriff „Zertifizierung" wird in der DS-GVO nicht definiert. Die Internationale Normungsorganisation (International Standards Organisation, ISO) versteht unter einer Zertifizierung allgemein die durch eine unabhängige Stelle erstellte schriftliche Versicherung (ein Zertifikat), dass ein in Frage stehendes Produkt, eine Dienstleistung oder ein System bestimmte Anforderungen erfüllt.[3] Als alternative Bezeichnung für Zertifizierung ist auch der Begriff „Konformitätsbewertung durch eine unabhängige Stelle" bekannt.[4]

Zur weiteren Festlegung dessen, was nach der DS-GVO zertifiziert werden kann, finden sich in der Verordnung selbst zusätzliche Hinweise. Aus Art. 42 Abs. 7 DS-GVO folgt, dass Zertifizierungen nach der DS-GVO ausschließlich Verantwortlichen und Auftragsverarbeitern erteilt werden dürfen. In Art. 43 Abs. 1 Buchstabe b DS-GVO wird auf die Norm ISO 17065 verwiesen, die die Akkreditierung von Zertifizierungsstellen vorsieht, welche die Konformität von Produkten, Dienstleistungen und Prozessen bewerten. Gegenstand der Zertifizierung nach Art. 42, 43 DS-GVO sind demnach Datenverarbeitungen in Produkten, Verfahren und Dienstleistungen.[5] Die Zertifizierung muss also immer eine konkrete Datenverarbeitung betreffen. Personen (etwa Datenschutzbeauftragte), Managementsysteme oder Konzepte können folglich nicht Zertifizierungsgegenstand sein. Dasselbe gilt für die Hersteller von Software, die nicht Verantwortliche oder Auftragsverarbeiter für Datenverarbeitungen sind. Sie können für ihre Produkte keine Zertifizierung nach DS-GVO erhalten.

Hierin liegt zugleich der größte Unterschied zwischen der Zertifizierung nach der DS-GVO und reinen ISO-Zertifizierungen. Zertifizierungen nach Art. 42, 43 DS-GVO können Klarheit darüber verschaffen, ob Verarbeitungsvorgänge den gesetzlichen Datenschutzanforderungen genügen. Zertifizierungen nach ISO/DIN haben eine andere Zielrichtung: Sie sind nicht maßgeschneidert auf den Datenschutz, sondern es geht immer um Managementsysteme, beispielsweise bei ISO 9001 (Qualitätsmanagement), bei ISO 27001 (Zertifizierung von Managementsystemen auf Basis von IT Grundschutz) oder in Verbindung mit ISO 27701 (deren Konformitätsaussage immer auf ein zertifiziertes Informationssicherheitsmanagementsystem gem. ISO 27001 beschränkt ist). Im Fokus stehen bei der ISO-Zertifizierung also nicht die Datenverarbeitungsvorgänge sondern die Systeme. Anders als bei der DS-GVO-Zertifizierung stehen nicht die Rechte und Freiheiten von betroffenen Personen im Mittelpunkt der Betrachtung. Selbstverständlich sind im Hinblick auf IT-Sicherheitszertifizierungen aber Synergieeffekte möglich.

Wer darf zertifizieren?

Um als Zertifizierungsstelle[6] nach der DS-GVO tätig werden zu können, muss sich eine Stelle zunächst für diese Tätigkeit akkreditieren lassen (Art. 43 DS-GVO). Eine Akkreditierung bestätigt, dass eine Zertifizierungsstelle die Kompetenz besitzt bestimmte Zertifizierungsverfahren durchzuführen und Zertifikate zu erteilen. Die Stelle

[2] Datenschutzaufsichtsbehörden könnten zwar auch selbst zertifizieren. Die meisten Behörden – auch die LDI NRW – tun dies aber nicht.
[3] Vgl. insoweit DIN EN ISO/IEC 17000:2020 "Konformitätsbewertung – Begriffe und allgemeine Grundlagen".
[4] Vgl. Leitlinie 1/2018 des Europäischen Datenschutzausschusses (EDSA) für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Art. 42 und 43 der Verordnung (EU) 2016/679, Version 3.0 vom 4.6.2019, Rn. 15, im Internet abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_de.
[5] So auch Leitlinie 1/2018 des EDSA für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Art. 42 und 43 der Verordnung (EU) 2016/679, Version 3.0 vom 4.6.2019, Rn. 55, wonach der Zertifizierungsbereich auf Verarbeitungsvorgänge bzw. Vorgangsreihen ausgerichtet ist. Im Internet abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_de.
[6] Zertifizierungsstellen werden auch als „Konformitätsbewertungsstellen" bezeichnet.

muss sich also zunächst selbst einer Überprüfung unterziehen, bevor sie zertifizieren darf.

In Deutschland werden Zertifizierungsstellen von der Deutsche Akkreditierungsstelle GmbH (DAkkS)[7] zusammen mit den Datenschutzaufsichtsbehörden des Bundes und der Länder akkreditiert (§ 39 BDSG). Für eine Akkreditierung als Zertifizierungsstelle muss eine Prüfung durchlaufen werden, die sich in zwei Teilbereiche mit insgesamt sechs Phasen untergliedert.[8]

Teilbereich eins (die sogenannte „Programmprüfung") besteht aus zwei Phasen. Neben der Fachprüfung des Programms erfolgt auch die Fachprüfung der Zertifizierungskriterien durch die zuständige Aufsichtsbehörde. Erfolgreich abgeschlossen wird die Fachprüfung der Aufsichtsbehörde mit der Genehmigung der Zertifizierungskriterien. Teilbereich zwei (die sogenannte „Akkreditierung") besteht insgesamt aus vier Phasen: Antrag, Begutachtung, Befugniserteilung und Überwachung. Die Akkreditierung ist auf höchstens fünf Jahre befristet (Art. 43 Abs. 4 DS-GVO). Vor Ablauf der Akkreditierung kann die Zertifizierungsstelle einen Antrag auf Verlängerung stellen.

Die Datenschutzkonferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in Abstimmung mit der DAkkS ergänzende Anforderungen zur DIN EN ISO/IEC 17065 für die Akkreditierung aufgestellt.[9] Solche Anforderungen sind in Art. 43 Abs. 3 DS-GVO vorgesehen. Einschlägige ISO-Normen wurden dabei berücksichtigt. Der Europäische Datenschutzausschuss (EDSA) hat zu den ergänzenden Anforderungen ebenfalls seine Stellungnahme angegeben.

Zertifizierungsprogramm und Zertifizierungskriterien

Zur Vorbereitung einer Akkreditierung müssen Zertifizierungsstellen bzw. Programmeigner*innen zunächst ein Zertifizierungsprogramm erstellen und durch die DAkkS auf Eignung prüfen lassen.[10] Wesentlicher Teil dieses Programms sind die Zertifizierungskriterien. Die Kriterien beschreiben den Anwendungsbereich des Programms, also für welche Verarbeitungstätigkeiten es angewendet werden soll. Sie müssen Vorgaben enthalten, an denen sich die Verarbeitungsvorgänge messen lassen. Darunter fällt unter anderem eine Beschreibung, wie das Zertifizierungsprogramm auf eine konkrete Zertifizierung ihrer Kund*innen angewendet werden soll (Target of Evaluation, ToE). Die Kriterien müssen außerdem einheitlich und nachprüfbar sein, also geeignet, um die Bewertung von Verarbeitungsvorgängen zu erleichtern. Insbesondere müssen Ziele definiert und Umsetzungshinweise zur Erreichung dieser Ziele gegeben werden. Die Kriterien müssen außerdem relevant und verständlich für den jeweiligen Adressatenkreis sein.

Zur Verdeutlichung, was die Aufsichtsbehörden im Rahmen ihrer Fachprüfung von den Antragstellern erwarten, haben die deutschen Aufsichtsbehörden einheitliche Anforderungen an Zertifizierungskriterien aufgestellt.[11] Das Papier richtet sich sowohl an Aufsichtsbehörden selbst als auch an Antragsteller*innen. Es gibt Hilfestellungen, was von Programmeigner*innen und Zertifizierungsstellen erwartet wird. Sie können sich schon bei der Erstellung ihrer Dokumente hieran orientieren. Erfahrungen und Erkenntnisse der Aufsichtsbehörden fließen weiterhin in die Anforderungen ein, die bei Bedarf angepasst werden. Das Papier zeigt zudem Interessierten, worauf es bei der aufsichtsbehördlichen Überprüfung ankommt.

Für eine Zertifizierungsstelle ist das Verfahren bis hin zur tatsächlichen Aufnahme ihrer Tätigkeit aufwendig. Prüfung und Kontrolle durch die Behörden schaffen aber zugleich Vertrauen in die Arbeit der Zertifizierungsstelle und in die erteilten Zertifikate für die Kund*innen. Sollte dennoch festgestellt werden, dass die Zertifizierungsstellen nicht vernünftig arbeiten, kann eine Akkreditierung auch wieder entzogen werden. Sämtliche akkreditierte Stellen werden in einem Verzeichnis bei der DAkkS geführt.

Praxistipp und Ausblick

Eine genaue Prognose, wann mit ersten DS-GVO-Zertifizierungen gerechnet werden kann, ist schwierig. Die LDI NRW hat zwei nationale Zertifizierungskriterien vorbehaltlich der Stellungnahme des EDSA für geeignet befunden. Nun stehen die Stellungnahmen des EDSA an (Art. 64 Abs. 1 Buchstabe c DS-GVO). Parallel dazu

[7] Die Deutsche Akkreditierungsstelle GmbH hat ihre rechtliche Grundlage im Akkreditierungsstellengesetz (AkkStelleG) gem. EU-VO 765/2008 und ist mit dieser Aufgabe beliehen.

[8] Übersicht: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Akkreditierung_Zertifizierung/Inhalt/Akkreditierung_Zertifizierung/20190315_oh_akk_c.pdf

[9] https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Akkreditierung_Zertifizierung/Inhalt/Akkreditierung_Zertifizierung/DIN17065-Ergaenzungen-deutsch-final_nach_Opinion_20201008.pdf

[10] Vgl. DAkkS-Regel 71 SD 0016, abrufbar unter: https://www.dakks.de/de/dokument-detail.html?id=regel-zur-pruefung-der-feststellung-der-akkreditierungsfaehigkeit-neuer-privater-konformitaetsbewertungsprogramme-gemaess-tz-4-6-3-en-iso-iec-1701171-sd-0-016.

[11] https://www.datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf.

laufen bereits die ersten Phasen der Akkreditierung bei der DAkkS. Weitere Anträge liegen in NRW vor. In anderen Bundesländern und EU-Mitgliedstaaten gibt es ebenfalls Pläne für Zertifizierungskriterien. Auch Europäische Datenschutzsiegel sind geplant.

Vorbehaltlich des weiteren Akkreditierungsprozesses könnten noch in diesem Jahr erste Zertifizierungsstellen in Deutschland datenschutzrechtliche Zertifizierungen nach der DS-GVO anbieten. Wenn diese Voraussetzungen geschaffen sind, geht es los und DS-GVO-Zertifizierungen für Verantwortliche und Auftragsverarbeiter sind dann möglich.

Interessierte Unternehmen, die Zertifikate erhalten möchten, sollten vor der Beauftragung einer Zertifizierungsstelle einen Blick in das Verzeichnis der akkreditierten Stellen bei der DAkkS[12] werfen. Nur so sind sie sicher, dass sie eine ordnungsgemäß akkreditierte Stelle beauftragen. Interessierte Unternehmen können einen Blick in die Zertifizierungskriterien der Zertifizierungsstellen und in das Papier „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ werfen. Dadurch ist leichter zu bestimmen, was überhaupt zertifiziert werden soll und wie die Zertifizierungsstelle prüfen wird.

Die komplexen Verfahren, bis eine Zertifizierung angeboten werden kann, und die umfassende Prüfung, bis ein Zertifikat erteilt wird, werden sich nach dem Konzept der DS-GVO auszahlen: Für die Inhaber von Zertifikaten – für Stellen, die gute Auftragsverarbeiter suchen – für Datenschutzbeauftragte, die guten Datenschutz prüfen – für die Aufsichtsbehörden – für die Anbieter von Programmen und Prüfungen – und nicht zuletzt für alle, deren personenbezogene Daten verarbeitet werden.

Über die Autorinnen

Bettina Gayk

ist seit Mai 2021 Landesbeauftragte für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen.
Zuvor war die Verwaltungsjuristin im Innenministerin in Düsseldorf stellvertretende Abteilungsleiterin.

Dr. Henrike Postberg

ist Referentin bei der LDI NRW im Referat Grundsatzfragen. Ihre Aufgabenschwerpunkte liegen in den Bereichen Verhaltensregeln und Zertifizierung.

▶ www.ldi.nrw.de

[12] Zu finden unter: https://www.dakks.de/de/akkreditierte-stellen-suche.html – Dort sind auch Stellen aufgeführt, die Zertifikate anbieten, die zwar einen Datenschutzbezug haben, aber keine DS-GVO-Zertifizierungen sind. Der Gegenstand der Akkreditierung sollte daher besonders beachtet werden.

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

„DATENSCHUTZ IST EIN SEISMOGRAPH DER RECHTSTAATLICHKEIT“

Ein Interview mit der neuen Sächsischen Datenschutzbeauftragten Juliane Hundert

Dr. Juliane Hundert trat zum Januar diesen Jahres ihr Amt als Sächsische Datenschutzbeauftragte an. Sie folgte auf Andreas Schurig, der 18 Jahre lang der Behörde vorstand. Mit der BvD-News sprach Juliane Hundert über ihre Ziele als Landesdatenschutzbeauftragte, welche Schwerpunkte sie setzen will und über die Überprüfung von Medienhäusern auf DSGVO-Tauglichkeit.

BvD-News: *Zunächst noch einen herzlichen Glückwunsch zu Ihrer Ernennung zur Sächsischen Datenschutzbeauftragten. Sie sind ja schon länger mit dem Thema Datenschutz betraut. Was hat Sie motiviert, sich des Themas anzunehmen?*

Juliane Hundert: Vielen Dank für die Glückwünsche! Ganz konkret zum Thema Datenschutz kam ich durch meine Arbeit als Referentin beim Sächsischen Datenschutzbeauftragten ab 2005. Allerdings war mir das Eintreten für die Rechte anderer schon immer ein Bedürfnis. Das zieht sich ein bisschen wie ein roter Faden durch mein Leben – mit meinem Engagement als Schulsprecherin, als Rechtsanwältin, als Referentin im Bereich des Sozialdatenschutzes und nicht zuletzt in meiner Arbeit als parlamentarische Beraterin in einer bürgerrechtlichen Partei.[1] Mich leitet dabei das Freiheitsversprechen des Grundgesetzes, dass auch die informationelle Selbstbestimmung der oder des Einzelnen umfasst. Von der DDR habe ich noch so viel erlebt, dass ich weiß, dass das staatliche Eindringen in unsere Privatsphäre Leben zerstören kann. Ich betrachte Demokratie und Rechtsstaat als großes Geschenk. Das motiviert mich. Und der Datenschutz – so meine Erfahrung – ist in unserer Demokratie ein Seismograf der Rechtsstaatlichkeit. Wenn ich mich für den Datenschutz einsetze, dann mache ich mich für unsere Grundrechte und unseren demokratischen Rechtsstaat stark.

BvD-News: *Welche Themen-Schwerpunkte haben Sie sich für Ihre Amtszeit vorgenommen?*

Juliane Hundert: Mein Haupt- und Herzensanliegen ist es Ansprechpartnerin für alle Bürgerinnen und Bürger im Freistaat Sachsen in Fragen des Datenschutzes zu sein. Ich möchte auch für transparentes Verwaltungshandeln eintreten, denn nicht selten werden Entscheidungen zu wenig erklärt und führen zu vermeidbaren Missverständnissen. Mit dem Transparenzgesetz, das derzeit im Sächsischen Landtag beraten wird, wird ein wichtiger Schritt zu mehr Bürgernähe gegangen. Als mögliche zukünftige Transparenzbeauftragte wird mein Aufgabenspektrum auf die Informationsfreiheit erweitert. Die Umsetzung dieses Gesetzes wird in den nächsten beiden Jahren auf jeden Fall ein Schwerpunkt sein. Darauf freue ich mich. Aber auch die Arbeit der Datenschutzbeauftragten muss transparenter werden. So sollen sich Bürgerinnen und Bürger, die Wirtschaft, Vereine und sonstige Stellen unkompliziert über datenschutzrechtliche Anforderungen und Lösungen informieren können. Ich möchte die Öffentlichkeitsarbeit meiner Behörde weiter ausbauen. Zudem möchte ich einen Schwerpunkt auf eine datenschutzfreundliche Gesetzgebung legen. Hier werden die Weichen für einen verhältnismäßigen Umgang mit dem Grundrecht auf informationelle Selbstbestimmung gestellt. Sind die Gesetze gut, ist es auch der Vollzug. So können schwere, ungerechtfertigte Eingriffe in unsere Grundrechte verhindert werden.

Mein Ziel ist es den Datenschutz als Selbstverständlichkeit unserer rechtsstaatlichen Ordnung auf allen Ebenen zu verankern. Datenschutz soll nicht mehr als Verhinderungsinstrument sondern als Wettbewerbsvorteil gesehen werden – sowohl im Vergleich zu anderen Gesellschaftsordnungen als auch für eine starke Wirtschaft.

BvD-News: *Im Juni 2021 wurde eine länderübergreifende Prüfung der Datenschutzaufsichtsbehörden zu Einwilligungen auf Webseiten von Medienunternehmen gestartet mit dem Schwerpunkt Nutzertracking zu Werbezwecken. Welche Erkenntnisse liegen Ihnen bislang vor?*

Juliane Hundert: Die Prüfung wird zwischen elf Aufsichtsbehörden koordiniert, findet aber im jeweiligen Zuständigkeitsbereich der örtlichen Aufsichtsbehörde statt. In Sachsen werden fünf reichweitenstarke Online-Angebote überprüft. Bis zum Jahresende 2020 wurden die umfangreichen Fragebögen von den Verlagshäusern beantwortet, im ersten Halbjahr 2021 wurden die Antworten ausgewertet und grundsätzliche Fragestellungen zwischen den beteiligten Behörden abgestimmt. Parallel hat meine Behörde mit allen Verlagshäusern Gespräche geführt. Thematisiert wurden dabei die Mechanismen der Einwilligungen, die Nutzung von Dienstleistern mit Datenexporten sowie generelle Fragestellungen von geeigneten Rechtsgrundlagen. Parallel fand in der Fachwelt die Diskussion rund um die Einführung des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) und dessen Auswirkungen auf die Praxis statt. Mit den Verlagshäusern konnten in einzelnen Punkten durchaus tragfähige Kompromisse erzielt werden. Gleichwohl wurde meine Behörde auf den hohen wirtschaftlichen Druck hingewiesen, der das Online-Mediengeschäft prägt. Die Prüfung ist noch nicht

abgeschlossen. Über ein Ergreifen aufsichtsrechtlicher Mittel kann ich zum jetzigen Zeitpunkt noch nicht befinden.

BvD-News: *In einem Interview im Januar dieses Jahres sagten Sie, „bei Gesundheitsdaten geht es ans Eingemachte". Was meinten Sie damit konkret?*

Juliane Hundert: Diese Aussage habe ich vor dem Hintergrund der umfangreichen Datenverarbeitung im Zusammenhang mit der Coronapandemie und der Frage getroffen, ob der Kampf gegen Corona den Datenschutz zurückgeworfen hat. Ich wollte verdeutlichen, dass viele unserer Daten, die in dieser Pandemie massenweise verarbeitet werden, Gesundheitsdaten sind, die besonders geschützt werden müssen. Bei der Frage nach dem Impfschutz, nach einer Infektion oder nach medizinischen Befunden geht es um zutiefst persönliche Angelegenheiten, die wir normalerweise nur mit unserer Ärztin besprechen, aber nicht mit unserem Arbeitgeber, den Lehrerinnen und Lehrern unserer Kinder oder unserer Buchhändlerin.

Mir ist aber bewusst, dass wir in der verhältnismäßig kurzen Geschichte des Datenschutzes noch keine Pandemie solchen Ausmaßes hatten. Und genauso wie die Frage des Umgangs mit dem Virus, stellt sich auch die Frage des Umgangs mit dem Datenschutz in der Pandemie immer wieder neu. Bei allen Maßnahmen gehört daher immer auch die Frage der Verhältnismäßigkeit auf den Tisch.

Fakt ist, dass die Erhebung und Speicherung von Daten in der Pandemie ein gigantisches Ausmaß erreicht hat. Es wäre vor wenigen Jahren unvorstellbar gewesen, dass ich beim Restaurant- oder Schwimmbadbesuch meine Adressdaten hinterlassen muss.

Umso wichtiger war es gesetzlich zu regeln, dass die Nutzung solcher Daten – etwa durch die Polizei – strikt beschränkt ist. Genauso wichtig ist es, dass diese Regelungen allesamt wieder aufgehoben werden, wenn sie zur Pandemiebekämpfung nicht mehr erforderlich sind.

BvD-News: *Welchen Stellenwert nimmt die Beratung von Unternehmen und von Datenschutzbeauftragten für Sie ein?*

Juliane Hundert: Das ist sehr wichtig! Je mehr wir als Datenschützerinnen und -schützer die Regeln des Datenschutzes und die Wichtigkeit des Grundrechts vermitteln, umso höher wird der Datenschutzstandard insgesamt und umso weniger Datenschutzverstöße müssen wir ahnden. Sehr gern würde ich diesen Bereich meiner Tätigkeit weiter ausbauen und mehr Informationsangebote unterbreiten. Allerdings muss ich mich dabei auf die wichtigsten Multiplikatoren konzentrieren, denn jedes einzelne Unternehmen und jede Datenschutzbeauftragte kann ich nicht beraten. Das ist nicht leistbar, so aber auch nicht gedacht.

BvD-News: *Die Ausstattung der Datenschutz-Aufsichtsbehörden ist immer wieder ein Thema – in allen Bundesländern. Welche Ausstattung wollen Sie für Ihre eigene Behörde erreichen?*

Juliane Hundert: Der Zuwachs an Aufgaben, der mit der Einführung der Datenschutzgrundverordnung auf die Aufsichtsbehörden zugekommen ist, ist schon enorm. Allein die Abstimmung mit den anderen Aufsichtsbehörden der Länder, des Bundes und der EU-Staaten erfordert sehr viel mehr Zeit als früher. Insgesamt sind die Anforderungen an so eine kleine Behörde wie meine extrem gestiegen. Es ist daher gut, dass der Haushaltsgesetzgeber im vergangenen Jahr dem Rechnung getragen und meiner Behörde acht neue Stellen eingerichtet hat. Die Zahl der Stellen stieg damit von 31 auf 39. Das ist großartig und – wenn ich die Kolleginnen und Kollegen in den anderen Ländern höre – nicht selbstverständlich. Noch sind nicht alle Stellen besetzt. Wenn das der Fall ist und sich die neuen Kolleginnen und Kollegen eingearbeitet haben, werde ich sehen, ob noch weiterer Bedarf besteht. Auf jeden Fall benötige ich für die neue Aufgabe als Transparenzbeauftragte weitere personelle Unterstützung.

BvD-News: *Und zum Schluss: Wie gehen Sie privat mit Cloud-Computing, Onlinebestellungen und Social Media um? Welche Auswirkungen Ihres Berufs bemerken Sie bei sich persönlich?*

Juliane Hundert: Da bin ich Endverbraucherin wie jede andere auch. Aber sicherlich eine kritische. Bestimmte soziale Medien und Messengerdienste nutze ich nicht. Wenn ich bestimmte Cookie-Einstellungen nicht abwählen kann, besuche ich die Seite nicht. Meine Familie verdreht immer die Augen, wenn ich bei Formularen nach der Rechtsgrundlage frage oder sage, nein, diese App nutzen wir nicht. Über eine Déformation professionnelle verfüge ich also definitiv.

Zur Person

Juliane Hundert

studierte in Jena Jura und promoviert 2009 dort in einem verbraucherschutzrechtlichen Thema. Im Anschluss absolvierte sie ein Referendariat am OLG Dresden und arbeitete als Rechtsanwältin. Von 2005 bis 2010 war sie Referentin beim Sächsischen Datenschutzbeauftragten. Ab 2011 bis zu Ihrer Wahl als Sächsische Datenschutzbeauftragte im Dezember 2021 war sie parlamentarische Beraterin der Grünen-Fraktion im Sächsischen Landtag mit den Schwerpunkten Innenpolitik, Kommunales, Datenschutz und Justiziariat.

Das Interview führte

Christina Denz

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

WERDEN DATENSCHUTZVERSTÖSSE IMMER TEURER?

Maria Christina Rost

2021 wurden die höchsten Bußgelder wegen Verstößen gegen die DS-GVO seit Geltung der DS-GVO verhängt. Werden Verstöße also immer teurer? Wohin geht die Reise 2022? Mit Spannung werden die Leitlinien des Europäischen Datenschutzausschusses Ende des Jahres erwartet.

Seit der Geltung der DS-GVO im Mai 2018 hängen die hohen Bußgeldern wie ein Damoklesschwert über den Unternehmen und natürlichen Personen. Die von den unabhängigen Datenschutzaufsichtsbehörden ausgesprochenen Bußgelder scheinen von Jahr für Jahr höher zu werden. 2018 lagen die höchsten verhängten Bußgelder in Deutschland noch bei 20.000 Euro. 2019 wurde die Millionengrenze überschritten. Das wohl bekannteste Bußgeld nach DS-GVO in Europa sind die von der französischen Aufsichtsbehörde CNIL verhängten 50 Millionen Euro gegen Google LLC. Der BfDI verhängte 9,55 Millionen Euro Bußgeld gegen eine Telekommunikationsdienstleiter und die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) gegen ein großes Immobilienunternehmen ein Bußgeld in Höhe von 14,5 Millionen Euro. Gegen beide Bußgelder wurde Einspruch eingelegt. Das Landgericht Bonn reduzierte das Bußgeld gegen den Telekommunikationsdienstleister auf 900.000 Euro (LG Bonn Urt. v. 11.11.2020 Az. 29 OWi 1/20 LG). Das Bußgeld gegen das Immobilienunternehmen wurde in erste Instanz aufgehoben und wird nach Einlegung der Beschwerde vor dem Kammergericht Berlin verhandelt. 2020 verhängte dann die britische Datenschutzbehörde ICO umgerechnet rund 22 Millionen Euro gegen British Airways und

20 Millionen Euro gegen die Hotelkette Mariott International – und trug damit schon den Umsatzausfälle im Zuge der Corona-Pandemie Rechnung. Denn zunächst waren die Bußgelder auf 204 Millionen Euro gegen British Airways und 110 Millionen Euro gegen Mariott taxiert worden. Der Hamburger Datenschutzbeauftragte verhängte 2020 außerdem rund 35 Millionen Euro gegen den Onlineshop der Modekette H&M.

2021 erreichen die Bußgelder wegen Verstößen gegen die DS-GVO bis dato unbekannte Höhen. Die Datenschutzaufsichtsbehörde in Luxemburg (CDNP) verhängte ein Bußgeld von 746 Millionen Euro gegen Amazon Europa Core S.à.r.l. und die irische Aufsichtsbehörde (DPC) 225 Millionen EUR gegen WhatsApp Ireland Ltd. Hinzukamen weitere Bußgelder der CNIL: 90 Millionen Euro gegen Google LLC und 60 Millionen Euro gegen Facebook Ireland Ltd und Google Ireland Ltd.

Neu war im vergangenen Jahr, dass mit dem Bußgeld gegen WhatsApp Irleand Ltd. der irischen Datenschutzaufsichtsbehörde der Europäische Datenschutzausschuss im Rahmen eines Streitbeilegungsverfahrens nach Art. 65 DS-GVO befasst wurde.

Das Bußgeld steht für die grenzüberschreitende Zusammenarbeit der Datenschutzaufsichtsbehörden in Europa und die Rolle des Kohärenzverfahrens für eine Harmonisierung der Bußgeld-Praxis. Wurde doch infolge des Streitbeilegungsverfahrens nach Art. 65 DS-GVO durch den Europäische Datenschutzausschuss ein verbindlicher Beschluss erlassen, der zur Folge hatte, dass das Bußgeld von einem Bußgeldrahmen zwischen 30 und 50 Millionen Euro nach Einwänden aus Deutschland, Frankreich, Italien, Niederlanden, Portugal, Polen und Ungarn auf letztlich 225 Millionen Euro heraufgesetzt wurde.

Der Streitbeilegungsbeschluss des Europäische Datenschutzausschuss nach Art. 65 DS-GVO vom 28. Juli 2021[1]gewährt einen Einblick in die Bußgeldpraxis der Aufsichtsbehörden. Außerdem zeigt er auf, dass das Kohärenzverfahren nach Art. 63 ff. DS-GVO einen bedeutenden Einfluss auf den Ausgang eines Bußgeldverfahrens nehmen kann. Einen Einfluss, der für die nicht am Verfahren Beteiligten kaum vorhersehbar ist. Mit dem Wissen, dass die Ermittlungen in dem Whats-App-Fall im Jahr 2018 aufgenommen wurden, ist anzunehmen, dass in den folgenden Jahren weitere hohe Bußgelder zu erwarten sind. Denn die aufwendigen Ermittlungen im Hintergrund können mehrere Jahre in Anspruch nehmen. Insbesondere kann das Verfahren dann länger dauern, wenn es sich um ein grenzüberschreitendes Verfahren handelt, in dem mehre Aufsichtsbehörden aus den Mitgliedstaaten zu beteiligen sind (Art. 60 ff. DS-GVO).

Mit großer Spannung werden die Leitlinien des Europäischen Datenschutzausschuss i.S. des Art. 70 Abs. 1 lit. k DS-GVO über die Festsetzung von Bußgeldern erwartet. Ausweislich dem im Einklang mit Artikel 29 der Geschäftsordnung des Europäischen Datenschutzausschuss erstellten zweijährigen Arbeitsprogramm für die Jahre 2021/2022[2] sind diese bis Ende 2022 zu erwarten. Unter der Säule II des Arbeitsprogramms sind zur Unterstützung der wirksamen Durchsetzung und der effizienten Zusammenarbeit zwischen den nationalen Aufsichtsbehörden Leitlinien für die Berechnung von Geldbußen vorgesehen. Bislang gibt es nur in einzelnen Mitgliedstaaten Leitlinien, wie beispielsweise das Bußgeldkonzept der deutschen Datenschutzkonferenz (DSK). Diese Leitlinien entfalten jedoch in den grenzüberschreitenden Fällen keine Relevanz. Den einzigen gemeinsamen europäischen Nenner im Zusammenhang mit Bußgeldern stellt bislang das Workingpaper 253 dar[3]. Darin sind Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der DSGVO formuliert, um eine einheitliche europaweite Praxis zu gewährleisten. Diese Leitlinien sind aus dem Jahr 2017. Der Ausschuss und die einzelnen Aufsichtsbehörden haben vereinbart, sie als gemeinsames Konzept zu verwenden. Dadurch soll ein einheitliches Vorgehen bei der Verhängung der Geldbußen sichergestellt werden, bei dem alle Grundsätze der vorliegenden Leitlinien gebührend berücksichtigt werden. Mit Ihnen hat sich der Ausschuss auf eine einheitliche Auslegung der Bewertungskriterien nach Art. 83 Abs. 2 DS-GVO verständigt.

Mit Neugier erwartet wird zudem, wann und wie der EuGH über eine der zentralen Fragen

[1] https://edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12021-dispute-arisen_en
[2] https://edpb.europa.eu/system/files/2021-03/edpb_workprogramme_2021-2022_en.pdf
[3] https://www.datenschutzkonferenz-online.de/media/wp/20171003_wp253.pdf

im Kontext mit den Bußgeldverfahren entscheidet. Das KG Berlin (Az.: 3 Ws 250/21 v. 06.12.2021) hat dem EuGH zwei Fragen zur Bußgeldhaftung von Unternehmen nach DS-GVO Verstößen vorgelegt. In den beiden Vorlagefragen geht es um die Frage, ob ein Bußgeld nach DS-GVO gegen ein Unternehmen auch ohne Feststellung eines konkreten Vorwurfs gegen eine natürliche Person verhängt werden kann (§ 30 Abs. 1 OWiG).

Die erste Frage lautet: Ist Art. 83 Abs. 4 bis 6 DS-GVO dahin auszulegen, dass es den Art. 101 und 102 AEUV zugeordneten funktionalen Unternehmensbegriff und das Funktionsträgerprinzip in das innerstaatliche Recht mit der Folge inkorporiert, dass unter Erweiterung des § 30 OWiG zugrundeliegenden Rechtsträgerprinzips ein Bußgeldverfahren unmittelbar gegen ein Unternehmen geführt werden kann und die Bebußung nicht der Feststellung einer durch eine natürliche und identifizierte Person, gegebenenfalls volldeliktisch, begangenen Ordnungswidrigkeit bedarf?

Die Zweite Frage lautet: Wenn die Frage zu 1. bejaht werden sollte: Ist Art. 83 Abs. 4 bis 6 DS-GVO dahin auszulegen, dass das Unternehmen den durch einen Mitarbeiter vermittelten Verstoß schuldhaft begangen haben muss (vgl. Art. 23 der Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Art. 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln), oder reicht für eine Bebußung des Unternehmens im Grundsatz bereits ein ihm zuzuordnender objektiver Pflichtenverstoß aus („strict liability“)? Die Entscheidung dieser beiden Frage könnte sich auf die Frage nach der Menge und Höhe von Bußgeldern auswirken.

Doch sollte bei Datenschutzverstößen gegen die DS-GVO nicht ausschließlich auf die Frage nach den Sanktionen abgestellt werden. Das wäre zu kurz gegriffen. Der Kontakt der verantwortlichen Stelle und des Auftragsverarbeiter mit der Aufsichtsbehörde beginnt bereits im Aufsichtsverfahren.

Die Bußgelder sind aufgrund ihrer Bekanntheit enger mit der Frage eines Datenschutzverstoßes verbunden. Über Bußgelder wird gesprochen. Ein Bußgeld stellt einen festgestellten Datenschutzverstoß noch nicht ab. Das kann nur die Verantwortliche Stelle von sich aus oder in Folge von Abhilfemaßnahmen der Datenschutzaufsicht nach Art. 58 Abs. 2 DS-GVO.

Über die Abhilfemaßnahmen der Datenschutzaufsicht erfährt die Öffentlichkeit aber in der Regel nur wenig. Über sie findet sich vielleicht ein Beitrag in den Tätigkeitsberichten der Datenschutzaufsichtsbehörden (Art. 59 DS-GVO), selten in der Presse. Die Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO können aber für die verantwortliche Stelle oder einen Auftragsverarbeiter empfindliche Folgen haben, die unter Umständen auch kostenintensiver und empfindlicher sein können als ein Bußgeld. Die Datenschutzaufsichtsbehörde kann den Verantwortlichen oder den Auftragsverarbeiter zum Beispiel anweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen (Art. 58 Abs. 2 lit. c DS-GVO). Darüber hinaus kann die Datenschutzaufsicht aber auch eine vorübergehende oder endgültige Beschränkung einschließlich eines Verbots verhängen (Art. 58 Abs. 2 lit. f DS-GVO). Dazu kommt die Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in ein Drittland oder an eine internationale Organisation (Art. 58 Abs. 2 lit. j DS-GVO). Eine Anordnung in den letzten beiden Konstellationen (Verbot und Untersagung) kann unter Umständen zu massiven Einschränkungen im Unternehmensbetrieb führen. Die Maßnahmen i.S. d. Art. 58 Abs. 2 DS-GVO werden mit Hilfe von Verwaltungszwangsmitteln durchgesetzt.

Den Behörden stehen die Zwangsmittel wie Ersatzvornahme, Zwangsgelder und unmittelbarer Zwang zur Verfügung. In der Regel wird die Behörde ein Zwangsgeld festsetzen, wenn die bloße Androhung keinen Erfolg zeigt. Ein Zwangsgeld kann bis zu einer Höhe von bis zu 25.000 Euro betragen. Zwar kann ein solcher Bescheid vor dem Verwaltungsgericht beklagt werden, allein schon deswegen, um den Eintritt der Rechtskraft des Bescheides zu verzögern. Das spielt aber für das Bußgeldverfahren erstmal keine Rolle. Die Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO schließen ein Bußgeld nicht aus. Nach Art. 58 Abs. 2 lit. i DS-GVO

kann eine Geldbuße nach Art. 83 DS-GVO zusätzlich oder anstelle von den in Art. 58 Abs. 2 DS-GVO genannten Maßnahmen verhängt werden, jenachdem wie die Umstände des Einzelfalls gelagert sind.

Insgesamt wird 2022 mit Blick auf mögliche Bußgelder ein spannendes Jahr werden. Rasselten die Datenschutzaufsichtsbehörden 2018/2019 noch mit den Säbeln, so wissen sie mittlerweile das Schwert mit scharfer Klinge zu führen. Für das laufende Jahr ist es nicht auszuschließen, dass neben der Verhängung von hohen Bußgeldern auch umfangreich von dem Kanon der Maßnahmen nach Art. 58 Abs. 2 DS-GVO Gebrauch gemacht werden wird. Vielleicht bislang zu leise, aber doch mit großen Schritten, haben die Aufsichtsbehörden die Aufsichtspraxis zu den Befugnissen in Art. 58 Abs. 2 DS-GVO implementiert. Es ist also nicht ausgeschlossen, dass Datenschutzverstöße höhere finanzielle Folgen haben, sei es durch verhängte Bußgelder oder sei es durch Anordnungen oder Anweisungen der Datenschutzaufsicht.

Über die Autorin

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

▶ https://datenschutz.hessen.de/

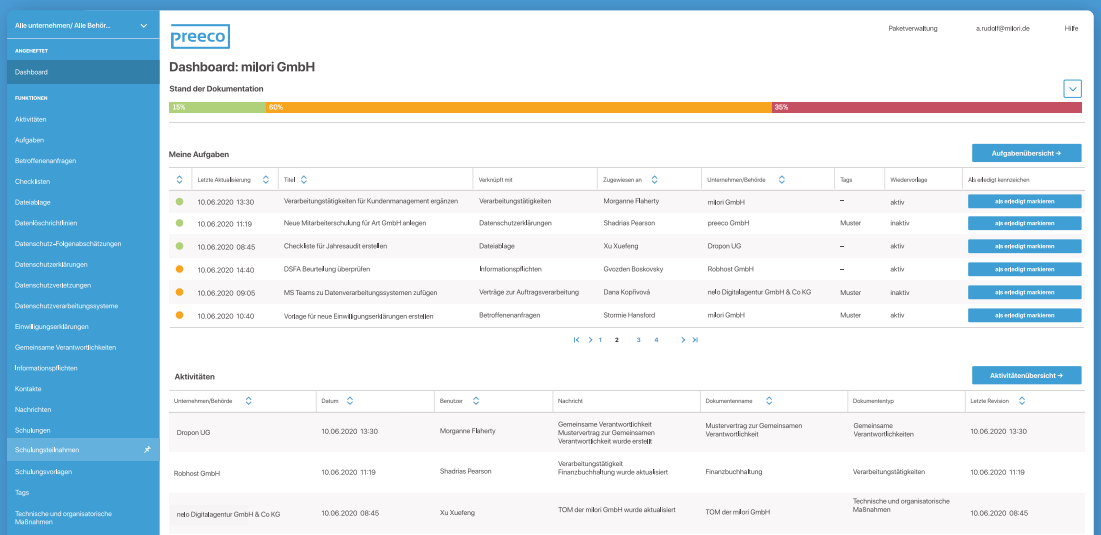
Anzeige

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



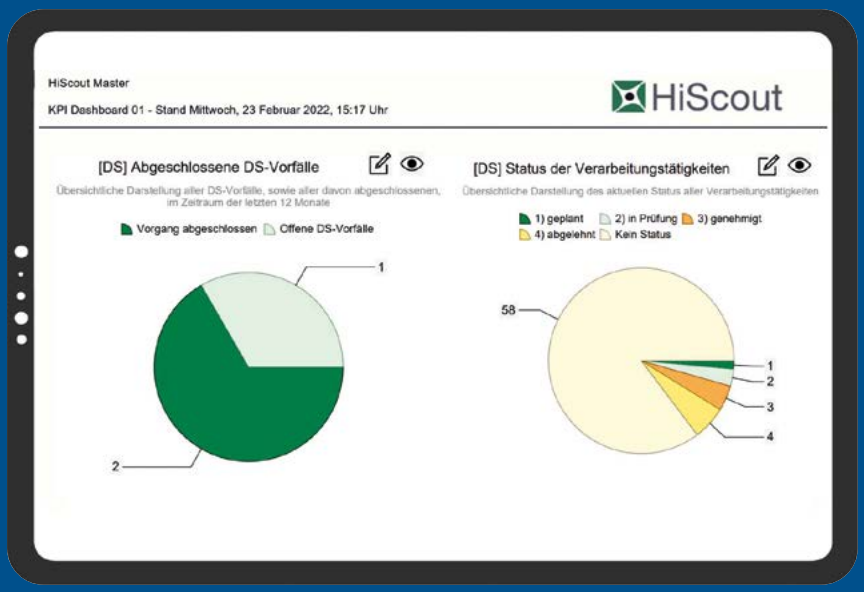
preeco GmbH
Magirus-Deutz-Straße 14
89077 Ulm
Telefon: +49 731 280 651 0
E-Mail: info@preeco.de
Web: **www.preeco.de**
Amtsgericht Ulm
HRB 737082
Geschäftsführer:
Andreas Hartmann

DATENSCHUTZSOFTWARE VON EXPERTEN FÜR EXPERTEN

Wirtschaftlicher und sicherer Datenschutz in einer Komplettlösung

Daniel Linder

Die Einhaltung der aktuellen Anforderungen des Datenschutzes muss heute, genau wie die Befolgung steuerlicher Vorgaben, eine Selbstverständlichkeit sein. Es ist höchste Zeit, diesen Bereich ebenso professionell und wirtschaftlich zu organisieren. Niemand kann sich den Mehraufwand, der durch unvollständige und qualitativ minderwertige Tools entsteht, auf Dauer leisten. Resultierende Fehler verursachen oft zusätzliche Kosten und beschädigen das Vertrauen in das Unternehmen. Am Beispiel der Komplettlösung HiScout Datenschutz zeigen wir Optimierungsmöglichkeiten für Funktionalitäten und Prozesse, die Datenschutzbeauftragten und Verantwortlichen bei der Evaluierung einer Datenschutzsoftware als Anregung dienen können.



Sichere Überwachung aller kritischen Datenschutzvorgänge auf einen Blick

Komplettlösung statt Stückwerk

Alle Anforderungen des Datenschutzes werden mit einem einzigen System abgedeckt. Dieses muss nicht um weitere Tools, Worddokumente und Exceltabellen ergänzt werden. Beispielsweise lassen sich auch Auftragsverarbeitungsverhältnisse und „Verarbeitungen mit gemeinsamer Verantwortung" erfassen und inklusive zugehöriger Dokumente revisionssicher aufbewahren.

Mandantenfähigkeit für große Organisation

Eine HiScout-Instanz kann hierarchische Strukturen mit Mandanten und Untermandanten abbilden. Infrastruktur, Stammdaten und Berechtigungssysteme werden zentral verwaltet und übergreifend genutzt.

Automatisierte Datenerhebung statt aufwendiger Einzelinterviews

Die HiScout Fragebogenvorlagen unterstützen den Datenschutzverantwortlichen bei der Befragung von Mitarbeitern und Dienstleistern über ihre Verarbeitungstätigkeiten. Die Fragebögen werden in einem automatisierten Prozess versandt, geprüft und in die HiScout-Datenbank eingelesen. Grundlegende Informationen und fachliche Erläuterungen werden kontextbezogen im Fragebogen selbst bereitgestellt. Zeitraubende mündliche Erklärungen sind nicht mehr nötig.

Workflow zur vollständigen Befüllung des VVT

Bei der Aufnahme des Verzeichnisses der Verarbeitungstätigkeiten werden die Anwender Schritt für Schritt durch die notwendigen Eingabemasken geleitet. Alle relevanten Punkte werden abgefragt, nichts wird vergessen.

Ausreichende Granularität des Datenmodells

Im Verarbeitungsverzeichnis werden alle Fakten der Verarbeitung personenbezogener Daten in vier Ebenen abgebildet: 1. Verzeichnis der Verarbeitungstätigkeiten, 2. Verarbeitungstätigkeit, 3. Datenart und 4. Datenobjekt. Dieses Grundgerüst ist die Voraussetzung dafür, dass nachfolgende Aufgaben wie Datenschutzfolgenabschätzungen, Löschkonzepte, Berichte für Datenschutzvorfälle und Auskunftsanfragen automatisiert ablaufen können. Ohne Betrachtung der datenschutzrelevanten Zusammenhänge auf Ebene der Datenarten ist die Erstellung eines Löschkonzeptes überhaupt nicht möglich!

Datenschutzfolgenabschätzung nach DSGVO oder SDM

Eine Schwellwertanalyse zeigt, ob eine Datenschutzfolgenabschätzung (DSFA) notwendig ist. Diese kann laut Empfehlung der Datenschutzkonferenz auch nach den Vorgaben des Standard-Datenschutz-Modells (SDM) durchgeführt werden.

Löschkonzept automatisch erstellen

Nach Hinterlegung von Lösch- und Aufbewahrungsfristen können Löschkonzepte erstellt und per Knopfdruck in einem Bericht zusammengefasst werden.

Auskunftsanfragen umgehend beantworten

Eine automatisierte Suchfunktion nach Betroffenengruppen zum Auffinden der Speicherorte personenbezogener Daten von Mitarbeitern, Kunden etc. ermöglicht schnelles Handeln, wenn es um die Wahrung der Betroffenenrechte geht.

Rechtssichere Abwicklung von Datenschutzvorfällen

Der HiScout Prozess zur Behandlung von Datenschutzvorfällen begleitet Sie bei der korrekten Erfassung und Verfolgung von Datenschutzpannen. Sie behalten die strengen Fristen für Meldungen an Behörden und Betroffene im Blick und ordnen geeignete Maßnahmen zu. Hinterlegte Zeitstempel belegen, dass der Vorfall DSGVO-konform behandelt wurde.

Alle benötigten Berichte auf Knopfdruck erstellen

Das Verzeichnis der Verarbeitungstätigkeiten und alle anderen Berichte zur Erfüllung der Nachweispflichten nach DSGVO können jederzeit minutenaktuell als PDF erstellt und an die entsprechenden Behörden oder Prüfstellen weitergeleitet werden. Ein einheitliches lesefreundliches Format erleichtert dem Prüfer die Arbeit.

Kostensenkung im Datenschutz

Der personelle Aufwand für Datenerhebungen, Analysen und die Überwachung von Datenschutzvorgängen verursacht hohe Kosten, die sich durch eine effektive softwarebasierte Abwicklung erheblich reduzieren lassen. Der von Routinetätigkeiten entlastete Datenschutzbeauftragte kann sich endlich auf die kritischen Fragestellungen konzentrieren.

Fazit

Mit der Komplettlösung HiScout Datenschutz bringen Sie Ordnung und Struktur in Ihr Datenschutzmanagement und können zugleich die Gesamtkosten reduzieren. Das komplett eigenständige Tool wurde von erfahrenen Datenschutzexperten direkt aus der Praxis für die Praxis konzipiert.

Über den Autor

Daniel Linder

Senior Consultant Datenschutz
Daniel Linder ist Datenschützer aus Leidenschaft mit vielseitiger Projekterfahrung als Datenschutzbeauftragter. Er war unter anderem als Ausbilder im Zertifizierungslehrgang des TÜV Thüringen tätig. Bei HiScout ist er für das Produktmanagement des Moduls HiScout Datenschutz verantwortlich.

▶ www.hiscout.com/webinar-datenschutz

HiScout

ANWENDUNGSSZENARIEN UND BEDENKEN BEIM EINSATZ KÜNSTLICHER INTELLIGENZ IN DER ÖFFENTLICHEN VERWALTUNG

Eine explorative Umfrage über den Einsatz künstlicher Intelligenz in Gemeinden.[1]

Wendy Heereman und Giusi Abagnale

Künstliche Intelligenz (KI) kann Städte, Kommunen und Gemeinden in Verwaltungsaufgaben und bei der Bearbeitung von Bürgeranfragen unterstützen. Doch wie verbreitet ist der Einsatz von KI-Systemen in den Verwaltungen? Eine explorative Umfrage von 14 Verwaltungen unterschiedlicher Städte untersucht, wie weit die Gemeinden bereits KI einsetzen, welche Bedenken sie dabei haben und für welche Anwendungsszenarien sie KI planen.

1. Digitalisierung und Einsatz von KI in der öffentlichen Verwaltung

Die öffentliche Verwaltung soll digitaler werden. So verpflichtet das Gesetz zur Verbesserung des Online-Zugangs zu Verwaltungsdienstleistungen (Online-Zugangsgesetz - OZG) die öffentliche Verwaltung, ihre Verwaltungsdienstleistungen bis Ende 2022 digital über Verwaltungsportale anzubieten. Darüber hinaus hat die Europäische Union beschlossen ein europäisches digitales Zugangsportal einzurichten.[2] Damit soll vor allem sichergestellt werden, dass bestimmte Verwaltungsverfahren grenzüberschreitend und diskriminierungsfrei angeboten werden. Die Umsetzung dieser Ziele in der vorgegebenen Zeit stellt die öffentliche Verwaltung vor große Herausforderungen, da einerseits die bestehenden Aufgaben weitergeführt werden müssen, andererseits aber auch Ressourcen benötigt werden, um die Digitalisierungsziele umzusetzen. Eine Möglichkeit die Digitalisierung der öffentlichen Verwaltung zu unterstützen, wird daher im Einsatz von KI gesehen. Durch künstliche Intelligenz soll erreicht werden, dass durch die Automatisierung intelligenten Verhaltens Menschen bei der Erfüllung von Aufgaben entlastet werden können.[3] Neben den bestehenden Chancen des Einsatzes von KI birgt dieser auch Risiken, zum Beispiel weil häufig große Datenmengen benötigt werden, um einen intelligenten Algorithmus – sozusagen in Vorbereitung auf seine spätere automatisierte Übernahme von Aufgaben – zu trainieren. Zu diesen Trainingsdaten können auch personenbezogene Daten zählen bei deren Verarbeitung in der Regel die Vorgaben des Datenschutzrechts zu beachten sind. Darüber hinaus kann die Verarbeitung personenbezogener Daten im Wirkbetrieb erforderlich sein, insbesondere wenn KI zur Vorprüfung von Bürgeranträgen eingesetzt wird, und KI-Entscheidungen zum Teil weitreichende Folgen für natürliche Personen haben, etwa wenn es um die Vorauswahl von Bewerbern um einen Arbeitsplatz geht.

Um unter Berücksichtigung der Chancen und Risiken den Einsatz künstlicher Intelligenz zu fördern, erstellte die Große Koalition im Anschluss an ein Konsultationsverfahren 2018 die „Strategie künstliche Intelligenz". Bereits in diesem Rahmen hatte sich die damalige Bundesregierung das Ziel gesetzt den Einsatz der KI für hoheitliche Aufgaben zu fördern. Damit wollte sie die *„zur Verbesserung von Effizienz, Qualität und Sicherheit von Verwaltungsdienstleistungen beitragen [und] Leistungen zielgerichteter, passgenauer und niedrigschwelliger für Bürgerinnen und Bürger sowie verwaltungsintern bereitstellen"*.[4]

Doch sind KI-Systeme aus heutiger Sicht in der öffentlichen Verwaltung bereits Realität und pla-

[1] Diese Forschungsarbeiten wurden vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

[2] Verordnung (EU) 2018/1724 des Europäischen Parlaments und des Rates vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Information, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) 1024/2012, ABl. 2018 L 295/1.

[3] Martini: Transformation der Verwaltung durch Digitalisierung, DÖV 2017, 443 (454).

[4] Strategie Künstliche Intelligenz der Bundesregierung, Stand: November 2018, https://www.bundesregierung.de/resource/blob/997532/1550276/3f7d3c41c6e056957412 73e78b8039f2/2018-11-15-ki-strategie-data.pdf, zuletzt abgebrufen am 10.11.2021, S. 31. Im Dezember 2020 wurde die Fortschreibung der KI-Strategie der Bundesregierung verabschiedet, die den Einsatz von KI in der öffentlichen Verwaltung ebenfalls fördert, siehe: https://www.ki-strategie-deutschland.de/files/downloads/201201_Fortschreibung_KI-Strategie.pdf., zuletzt abgerufen am 09.12.2021, S. 23-24.

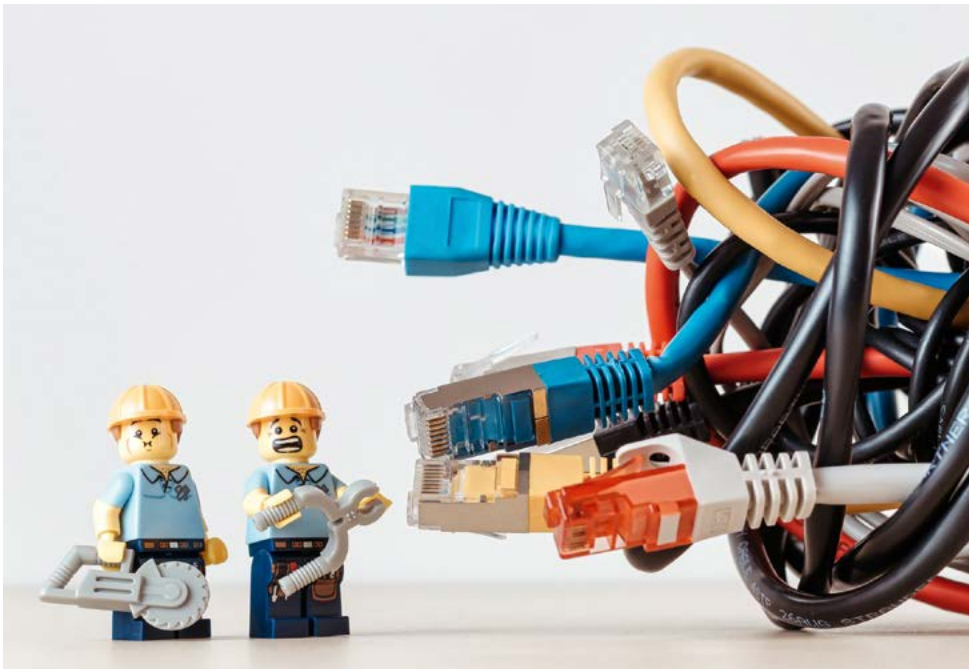
nen Gemeinden sie in der Zukunft verstärkt einzusetzen? Im Rahmen einer explorativen Datenerhebung im Herbst 2021 wurden 14 Gemeinden hierzu befragt, davon sieben kleine bis mittelgroße Städte[5] (nachfolgend Gruppe 1) und sieben Großstädte[6] (nachfolgend Gruppe 2). Befragt wurden die IT-Verantwortlichen, teilweise vertreten durch die datenschutzrechtlichen Verantwortlichen oder durch die externen IT-Dienstleister der jeweiligen Gemeinde. Ziel der Befragung war es den Umsetzungsstand und Bedenken zum Einsatz von KI in der öffentlichen Verwaltung zu erfragen (Abschnitt 2) sowie KI-Anwendungsszenarien zu identifizieren (Abschnitt 3). Die Ergebnisse der explorativen Befragung werden im Folgenden skizziert.

2. Einsatz von KI in der öffentlichen Verwaltung: Umsetzungsstand und Bedenken

Zunächst wurden die Gemeinden gefragt, ob sie bereits zum jetzigen Zeitpunkt KI-Systeme einsetzen. Diese Frage konnten sechs der 14 befragten Gemeinden bestätigten, von denen vier zu der Gruppe 2 (Großstädte) zählen. Von den verbleibenden acht Gemeinden gaben fünf an, dass sie die Einführung von KI-Systemen kurz- bis mittelfristig planen. Ebenso planen fünf der sechs Gemeinden, die bereits KI einsetzen, den Einsatz von KI kurz- bis mittelfristig zu erweitern.

Die drei Gemeinden, die sowohl den bisherigen Einsatz als auch die Planung von KI in ihrer Verwaltung verneinten, wurden nach den Gründen hierfür befragt. Genannt wurden unter anderem mangelnde Überzeugungsarbeit innerhalb der Verwaltung sowie fehlendes Wissen über künstliche Intelligenz und damit verbundener Schulungsbedarf. So sei es nötig zunächst Entscheidungsträger und Mitarbeiter von den Vorteilen der KI zu überzeugen und insbesondere diejenigen Mitarbeiter technisch zu schulen, die es gewohnt sind mit physischen Dokumenten zu arbeiten, um alle Mitarbeiter auf den gleichen technischen Wissens- und Verständnisstand zu bringen.

Besonders häufig wurden die Umsetzung des Datenschutzrechts und das fehlende Vertrauen in die KI als Grund für die Nichtdurchführung oder Planung von KI-Projekten erwähnt. So sei KI eine neue Technologie, die noch mit Problemen behaftet sei, darunter die Herausforderung die gesetzlichen Transparenzanforderungen zu gewährleisten. Eine Entscheidungsfindung durch KI sei zudem nicht transparent genug, um hoheitliche Aufgaben ausführen zu lassen. Zudem seien KI-Systeme nicht fehlerfrei und könnten insbesondere nicht alle kontextbezogenen Umstände berücksichtigen und daher keine Ausnahmen einbeziehen.



3. Einsatz von KI in der öffentlichen Verwaltung: Anwendungsszenarien

I. Chatbots als derzeitiges Hauptanwendungsszenario

Als aktuelles Hauptanwendungsszenario der KI in der öffentlichen Verwaltung konnten Chatbots identifiziert werden: Drei der sechs Gemeinden, die bereits KI-Systeme verwenden, setzen einen Chatbot ein, vier der acht Gemeinden, die derzeit den Einsatz von KI-Systemen vorbereiten, planen den Einsatz eines Chatbots.

a) Funktionsweise und Einsatzbereich

Chatbots sind KI-basierte Softwareanwendungen, die in der Lage sind eine Online-Konversation zu führen und bestimmte Standardfragen selbstständig zu beantworten.[7] In der öffentlichen Verwaltung eignen sich Chatbots besonders für die Kommunikation mit dem Bürger. Mit Hilfe eines

[5] Städte und Gemeinden unter 100.000 Einwohner.
[6] Städte und Gemeinden ab 100.000 Einwohner.
[7] Guggenberger: Einsatz künstlicher Intelligenz in der Verwaltung, NVwZ 2019, 844 (848).

Chatbots, welcher auf den Verwaltungs-Webpages integriert ist, können die alltäglichen Fragen der Bürger jederzeit beantwortet werden, unabhängig von den Öffnungszeiten der Verwaltung und ortsunabhängig.

In der öffentlichen Verwaltung bieten Chatbots eine erste Orientierung zu ihrem jeweiligen Anliegen, stellen ausgewählte Informationen zur Verfügung und können unter anderem das Bestehen von Ansprüchen, etwa auf Grundsicherung oder Arbeitslosengeld, prüfen.[8] Chatbots können ebenfalls Fragen in verschiedenen Sprachen verstehen und beantworten und dadurch nicht-deutschsprachige Bürger bei der Erledigung von Verwaltungsvorgängen unterstützen.

Gleichzeitig entlasten die Chatbots die Mitarbeiter der Verwaltung, indem sie wiederkehrende Fragen und Vorprüfungen von Anträgen übernehmen.

b) Transparente Verarbeitung personenbezogener Daten

Bei der Kommunikation mit einem Chatbot können verschiedene personenbezogene Daten anfallen, darunter IP-Adresse, Name, Wohnanschrift, Alter, Familienstand, Informationen über die wirtschaftliche Situation einer betroffenen Person und – zum Beispiel bei der Prüfung eines Anspruchs auf einen Behindertenausweis – allgemeine Gesundheitsdaten. Werden personenbezogene Daten bei dem Einsatz von Chatbots verarbeitet, so müssen die Datenschutzvorschriften insbesondere der DSGVO eingehalten werden. Der Verantwortliche ist unter anderem verpflichtet, die Transparenz und Nachvollziehbarkeit der Verarbeitung zu gewährleisten (Art. 12 -15 DSGVO).

Dazu gehört die Bereitstellung von Informationen über den Gegenstand und den Umfang der Datenverarbeitung, die Rechtsgrundlage für die Verarbeitung, die Empfänger der Daten und über das Vorliegen einer automatisierten Entscheidungsfindung. Darüber hinaus müssen Informationen über die Rechte der betroffenen Person zur Verfügung gestellt werden.

II. Weitere Anwendungsszenarien

Neben dem (geplanten) Einsatz von Chatbots nannten die befragten Gemeinden zudem weitere KI-Anwendungen, die entweder bereits zum jetzigen Zeitpunkt eingesetzt werden oder für die zukünftige Nutzung eingeplant[9] sind. Besonders häufig wurde der Einsatz von KI für das Erkennen und das Abwehren von Angriffen auf die IT-Systeme der öffentlichen Verwaltung genannt. Dies dient dem Zweck die Datenbanken, Rechner und sämtliche behördlichen Informationen vor Hackerangriffen zu schützen. Als weitere relevante Anwendungsfelder von KI in der öffentlichen Verwaltung konnten darüber hinaus insbesondere die KI-gestützte Parkraumsteuerung zur Auslastungskoordination der städtischen Parkflächen, Hinweisgebersysteme zur Meldung und KI-gestützten Koordination von Störungen wie kaputten Ampeln sowie KI-gestützte Auswertung von Videoüberwachungsanlagen auf öffentlichen Plätzen identifiziert werden.

[8] Siehe z.B.: https://www.arbeitsagentur.de/vor-ort/ingolstadt/die-ba-entwickelt-chatbots-fur-jede-lebenslage.

[9] In diesem Sinne wurde erfragt, ob in naher oder ferner Zukunft KI-Systeme bereits geplant sind oder zumindest eine Idee zum Einsatz besteht.

4. Zusammenfassung

Die explorative Befragung zeigte, dass bereits sechs der 14 befragten Gemeinden KI-Systeme einsetzen und weitere fünf Gemeinden den Einsatz von KI kurz- bis mittelfristig planen. Besonders häufig werden bereits Chatbots eingesetzt oder deren Einsatz geplant. Weitere mögliche Anwendungsfelder von KI-Systemen bestehen für die Abwehr von Angriffen auf die IT-Systeme, für die Steuerung von Parkleitsystemen, für die Reaktion auf Hinweisen im Rahmen der Bereitstellung von Hinweisgebersystemen und für die Auswertung von Videoüberwachungen. Bedenken zum KI-Einsatz in der öffentlichen Verwaltung gibt es insbesondere noch in Bezug auf die datenschutzkonforme Nutzung und speziell in den Bereichen der Transparenz. Des Weiteren wurden fehlendes Fachwissen sowie mangelnde Überzeugungsarbeit als Hemmschuhe des KI-Einsatzes in der öffentlichen Verwaltung genannt. Es ist davon auszugehen, dass fehlendes Fachwissen und mangelnde Überzeugungsarbeit bedingende Hintergründe in der Förderung des KI-Einsatzes in der öffentlichen Verwaltung sind und daher in den Aufbau des entsprechenden Fachwissens investiert werden sollte. Für den weiteren Ausbau des KI-Einsatzes in der öffentlichen Verwaltung werden darüber hinaus Lösungen für einen transparenten und vertrauenswürdigen KI-Einsatz benötigt.

Über die Autorinnen

Wendy Heereman

ist wissenschaftliche Mitarbeiterin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Darmstadt

Giusi Abagnale

arbeitet als studentische Mitarbeiterin am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) in Darmstadt.

▶ www.sit.fraunhofer.de

Fraunhofer SIT

Anzeige

2B Advice®
The Privacy Benchmark

Mit 2B Advice Datenschutzlösungen haben Sie ein Problem weniger.

DSFA / PIA / Risikoanalyse und -bewertung, Aufzeichnungen von Verarbeitungstätigkeiten (RoPA), Verarbeitungsübersicht und Datenflüsse, Management von Verarbeitungen & Berichterstellung, Datenschutz Compliance Check, Vorlagen, Assistenten und Kataloge, Verwaltung von Betroffenenanfragen, Integrierte webbasierte Trainingsplattform, Integrierte Onlinekommunikation, Mehrsprachigkeit, Planung und Berichterstattung, Webseiten Analyzer, Cookie Policy Generator, Privacy Statement Generator, Consent Manager, Web Services & REST-API

Bestellen Sie unsere KOSTENLOSE Einzelplatzversion

2B Advice GmbH - the privacy benchmark | Joseph-Schumpeter-Allee 25, Bonn
0228 926165-100 | sales.de@2b-advice.com | www.2b-advice.com

TÜV SÜD ISO 27001

2B Advice ist ISO/IEC 27001:2013 zertifiziert

"UUUND ACTION!" FÜR „DATENSCHUTZ GEHT ZUR SCHULE“

BvD-Initiative produziert 18 Clips für Schüler:innen und Lehrkräfte

Rudi Kramer

Katarina Leikert von der BvD-Initiative "Datenschutz geht zur Schule"

Nachdem auch die Vorträge zum Safer Internet Day 2021 wegen der Corona-Pandemie ausgefallen waren, kam uns die Idee: Gemeinsam mit dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW), Dr. Stefan Brink, wollten wir Kinder und Jugendliche im Homeschooling auch weiterhin mit Videos zum Thema Datenschutz erreichen. Heraus kamen 18 Clips, die über Datenschutz und Datensicherheit auf der neuen Website datenschutz-leicht-erklaert.de informieren.

Dr. Lutz Hasse,
Thüringer Datenschutzbeauftragter:
„Auch bei der Lehrerausbildung gibt es im Bereich Medienkompetenz oft gro ße Lücken, obwohl sie fester Bestandteil der Studienpläne ist. Die Videos sind daher kleine Lichtblicke bei der Vermittlung des bisweilen etwas sperrigen Themas Datenschutz, sowohl für die Schüler:innen als auch für die Lehrkräfte. Sie zeigen zudem anschaulich, dass viele engagierte Akteure etwas auf die Beine stellen können – möglicherweise ein Modell zur Lösung einiger Probleme in diesem Bereich.“

Vom LfDI BW unterstütze uns vor allem Martina Strifler im Rahmen ihres Aufgabenbereiches „Datenschutz als Kulturaufgabe“ engagiert bei der Organisation und der Abstimmung mit den Aufsichtsbehörden, die wir als Partner gewinnen wollten. Da mussten Ideen vorgestellt, die Pläne zur Umsetzung erläutert und geklärt werden, ob die Ressourcen dafür ausreichten. Am Ende sagten neben dem LfDI BW das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) und der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit (TLfDI) zu.

Miriam Meder vom Bayerischen Landesamt für Datenschutzaufsicht

Gemeinsam mit engagierten Datenschutzbeauftragten unserer Initiative ging es dann in die Planung.

Der Bundesbeauftragte für den Datenschutz und die Informatiomsfreiheit (BfDI) stellte uns für die Abstimmungen sein Videokonferenztool bereit.

Professsor Alexander Roßnagel,
Hessischer Datenschutzbeauftragter:
„Datenschutz ist wenig greifbar und sehr komplex. Daher ist es sehr verdienstvoll, wenn junge Menschen bereits in der Schule oder in der Ausbildung in einer für sie verständlichen Form an das Thema herangeführt werden und einfache Mechanismen und einfache rechtliche Regelungen im Umgang mit dem Datenschutz erfahren“.

"DSgzS" klärt auf - in 18 Videos zu allen Themen, die Jugendliche beschäftigen

Weitere Akteure gewannen wir aus den Reihen der DSgzS-Dozent:innen. Mit dabei sind die Datenschutz-Fachleute und BvD-Mitglieder Katarina Leikert, Melanie Schoch, Frank Spaeing und Dirk Wolf sowie die zwölfjährige Enya. Von Seiten der Aufsichtsbehörden wirkten Gernot Besant (HBDI), Sabine Pöllmann und René Rösel (TLfDI), Miriam Meder und Dr. Mirka Mölder (BayLDA) sowie Dr. Walter Kicherer und Dr. Stefan Brink vom LfDI BW mit.

Frank Spaeing von der BvD-Initiative "Datenschutz geht zur Schule"

Dr. Stefan Brink,
Datenschutzbeauftragter von Baden-Württemberg und Mitiniator der Videoreihe:
„Junge Menschen bewegen sich in der digitalen Welt gekonnt. Wir unterstützen Schüler:innen dabei sich mit der Digitalisierung intensiv zu befassen. In kurzen Videoclips zeigen wir leicht verständlich, wie sie sich und ihre persönlichen Daten einfach und mit wenig Aufwand besser schützen können. Eltern und weitere Betreuungspersonen können diese Clips nutzen, um leicht verständlich über Digitalisierung und Datenschutz zu sprechen."

Die Produktion lief an zwei Tagen im Spätherbst 2021 in einem angemieteten Studio in Frankfurt am Main unter 2Gplus, also „geimpft" oder „genesen" und zusätzlich jeden Tag einen Corona-Test. Natürlich mussten wir Sequenzen wiederholen und nochmals wiederholen und improvisieren, aber das trug auch zur Spontanität bei.

Schnell waren die Themen verteilt. Bei der Organisation waren Katrin Eggert und Nadja Bunk eine unverzichtbare Hilfe. Die Arbeit in Zweierteams half uns Feedback auf erste Video-Ideen zu bekommen. Eine wertvolle Unterstützung gab es bereits in dieser Phase durch das Kreativnetzwerk „Zeitgenossen", die frühzeitig auf die technischen Realisierungsmöglichkeiten hinwiesen.

Michael Will,
Präsident des Bayerischen Landesamts für Datenschutz:
„Während der Pandemie können wir nur eingeschränkt selbst in die Schulen kommen. Die Videos füllen diese Lücke. Schüler:innen können sich selbst durch die Videos klicken, um zu lernen, wie sie sich im Netz schützen. Lehrer:innen erhalten Unterrichtsmaterial, um die wichtigsten Themen zu besprechen."

Die Videos wollen Jugendliche dafür sensibilisieren mehr auf Datenschutz in sozialen Netzwerken, beim Selfie-Posten und Fotografieren, im Umgang mit Webcams, Smartphones und Drohnen zu achten und Passwörter sicher zu vergeben. Außerdem geben die Clips Hinweise für Berufsschüler:innen zum Einsatz bei Berufsgeheimnisträgern, klären über Datenschutzrechte in der Schule und auf der Arbeit auf und warnen vor Sexting und Profiling.

Die Videos werden mit Untertitel versehen und können dadurch barrierefrei genutzt werden. In Abstimmung mit unserem Partner klicksafe sind zu einigen Clips Arbeitsblätter vorgesehen, um sie noch zielgruppenpassender einsetzen zu können. Wer Zweifel haben sollte, dass Maßnahmen zur Datenschutzsensibilisierung keinen Spaß machen können, kann sich durch das Video zum „Making of" vom Gegenteil überzeugen lassen.

Walter Kicherer arbeitet beim Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (Foto: Zeitgenossen)

Die Resonanz nach der Veröffentlichung bestärkt uns bei DSgzS, auf diesem Weg weiterhin Jugendliche anzusprechen. Wer sich engagieren möchte, ist herzlich Willkommen. Wir freuen uns auch über Geldspenden an die gemeinnützige Gesellschaft privacy4people, die die Arbeit der BvD-Initiative DSgzS trägt. Die Videos wurden durch eine Förderung der DATEV Stiftung Zukunft ermöglicht.

Die 12-jährige Enya unterstützt die BvD-Initiative "Datenschutz geht zur Schule"

Die Video-Clips sind über www.datenschutz-leicht-erklaert.de abrufbar.

Alle Videos sind unter der Creative-Commons-Lizenz CC BY NC ND 4.0 veröffentlicht, das heißt, sie dürfen unter Nennung des Urhebers veröffentlicht, nicht aber verändert oder kommerziell eingesetzt werden.

Über den Autor

Rudi Kramer
ist Sprecher der BvD-Initiative „Datenschutz geht zur Schule" (DSgzS) und selbst Mitwirkender in einigen Videos.

Die Mitwirkenden der 18 Videos. (Foto: Zeitgenossen)

Anzeige

Steckt auch in Ihnen die **Service-DNA**?

Dann verbinden Sie sich jetzt mit dem größten Service-Netzwerk Europas*:

Werden Sie Mitglied im Service-Verband KVD e. V. und profitieren Sie neben dem professionellen Netzwerk mit den Verbindungen in Praxis, Forschung und Politik auch von der internationalen Zusammenarbeit des KVD, zum Beispiel mit dem österreichischen Verband KVA und dem Schweizer Pendant, dem SKDV.

Informieren Sie sich jetzt unter **www.kvd.de**.

* Der KVD gilt mit seinen 1.600 Mitgliedern als größtes verbandliches Service-Netzwerk seiner Art in Europa. Er unterstützt Fach- und Führungskräfte bei der Gestaltung ihres technischen Kundendienstes. Über Netzwerkveranstaltungen, Aus- und Weiterbildungen sowie die Einbindung neuester Forschungsergebnisse erhalten Mitglieder einen entscheidenden Wissens- und damit Marktvorsprung.

DATENSCHUTZ IST GELUNGENE KOMMUNIKATION

Der Daten-Dienstag im Museum für Kommunikation Nürnberg begeht seine 50. Ausgabe

Dr. Vera Losse

Der Journalist und Blogger Richard Gutjahr sprach im Jahr 2019 zum Thema: "Datenmacht und Datenmissbrauch - mehr Datenschutz jetzt" Foto: Vera Losse

Am 28. Juni 2022 findet der Daten-Dienstag, eine besondere Vortragsreihe im Museum für Kommunikation Nürnberg, zum 50. Mal statt. Diese erfolgreiche Veranstaltungsreihe wurde im Jahr 2015 von Rudi Kramer, damals Vorstandsmitglied im BvD, zusammen mit Marion Grether, der früheren Direktorin des Museums, initiiert. Wie kam es zu der Idee für dieses Format, das mittlerweile im achten Jahr stattfindet?

Die DSGVO trat am 24. Mai 2016 in Kraft und regelt nach einer zweijährigen Übergangsphase seit dem 25. Mai 2018 den datenschutzrechtlichen Rahmen innerhalb der Europäischen Union. Dieser Verordnung ging ein langer Abstimmungs- und Diskussionsprozess voraus, der mit dem ersten Entwurf der EU-Kommission aus dem Jahr 2012 begann. Heute ersetzt die DSGVO die aus dem Jahr 1995 stammende erste EU-Datenschutzrichtlinie und reagiert umfassend auf die zunehmende Digitalisierung von Privatleben, Wirtschaft und Gesellschaft.

Das 20-jährige Jubiläum der Europäischen Datenschutzrichtlinie aus dem Jahr 1995 war der ursprüngliche Anlass, die Vortragsreihe „Daten-Dienstag" ins Leben zu rufen. Initiator Rudi Kramer erinnert sich: „Die damalige Neugestaltung des Internet-Bereichs im Museum für Kommunikation Nürnberg rund um das Thema digitale Kommunikation lud ein dies als Hintergrund für ein Informations- und Diskussionsformat zur damaligen Entstehung der DSGVO zu nehmen. Denn außerhalb der Fachwelt erfuhr dies keine Resonanz in den Medien, obwohl schon absehbar war, welchen Einfluss sie haben würde. Es war das Ziel ein Format zu entwickeln, welches Themen rund um Internet und Privatheit in einer Form aufgreift, die sowohl die interessierte Öffentlichkeit erreicht als auch fachspezifischen Anforderungen standhält." Für das Museum war das Angebot interessant, so die damalige Direktorin Marion Grether, „weil der digitale Alltag viele neue Chancen zur Vernetzung und zur Informationsgewinnung bietet, und das wiederum erfordert Medienkompetenz. Aus diesem Grund haben wir 2015 den Daten-Dienstag etabliert."

Ursprünglich sollte das Angebot nur im Jahr 2015 stattfinden. Damals startete die Reihe am 13. Januar 2015 mit einem Vortrag von Prof. Dieter Kempf, dem damaligen Präsidenten des Branchenverbandes BITKOM, der zugleich Vorstandsvorsitzender der DATEV eG war. Sein Thema lautete: „Sind Daten die Währung von morgen?". Aufgrund der positiven Publikumsresonanz im ersten Jahr und der Vielzahl der Themen, die sich rund um den überlegten Umgang mit Daten im Netz seither ergeben haben, wird der Daten-Dienstag nun schon im achten Jahr veranstaltet. Trotz der weiten inhaltlichen Spanne und der ganz unterschiedlichen Referentinnen und Referenten, die seither Vorträge gehalten haben, ist das Ziel immer das Gleiche geblieben: Fakten rund um die Themen Datenschutz und Datensicherheit auch an Nichtfachleute zu vermitteln.

Seit 2018 ist mit dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) ein weiterer Kooperationspartner hinzugekommen. Thomas Kranig, der damalige Präsident des Landesamtes, sah hier eine gelungene Möglichkeit die Arbeit seiner Behörde einer breiten Öffentlichkeit vorzustellen. Er erinnert sich: „Mich motivierte damals und während meiner gesamten Tätigkeit im BayLDA der Wunsch den Leuten auf der Straße den Datenschutz verständlich zu machen und dafür zu werben, dass es dabei nicht um einen überzogenen Bürokratismus geht, sondern um Grundrechtsschutz im Interesse und zum Nutzen von uns allen. Mein Ziel war, dass ‚die Leute' verstehen, was wir machen, warum wir etwas machen und eventuell auch

wie wir es machen – und das kam bei den meisten Daten-Dienstagen hervorragend zum Ausdruck, zum Beispiel beim Schufa-, Payback- oder auch bei meinem Vortrag zu Bildern im Netz. Schön war dabei auch die direkte Diskussion mit dem Publikum, die derzeit nicht möglich ist".

Auch Michael Will, der Kranig 2020 an der Spitze des BayLDA nachfolgte, zeigte von Beginn an großes Engagement für das Format. Er konstatiert eine sehr hohe Daten-Sensibilität in der Bevölkerung und verweist auf Debatten, die in anderen Ländern nie stattgefunden haben, etwa über den Datenaustausch mit den USA, das Swift-Abkommen, das Acta-Abkommen zum Urheberrecht oder Datenschutzaspekte bei Handelsabkommen wie CETA oder die Debatte um die Corona-App. Die Menschen erwarten und verteidigen diesen besonderen Freiheitsraum.

Einen weiteren Entwicklungsschritt hat der Daten-Dienstag unter dem Einfluss von Corona gemacht: Seit Juli 2020 gibt es den Daten-Dienstag digital. Die ersten Termine fanden statt, als die Museen zwar eingeschränkt wieder öffnen konnten, aber Veranstaltungsbesuche nicht möglich waren. Dr. Annabelle Hornung, seit Juni 2020 Direktorin des Hauses, betont, dass ihr das Thema Datenschutz als Bestandteil der gelungenen Kommunikation sehr wichtig ist, denn „wir zeigen im Museum die Entwicklung der Kommunikation, dazu hat auch immer das Thema Datenschutz und Vertraulichkeit wie etwa das Briefgeheimnis, gehört.

Mit der Entwicklung digitaler Kommunikationstechnologien ist der Wunsch Daten zu schützen, gestiegen, gleichzeitig werden die damit verbundenen Probleme immer komplexer. Insofern existiert zwischen dem Bestreben eine möglichst einfache Kommunikation zu ermöglichen und dabei Vertraulichkeit und Integrität zu sichern, oft ein Spannungsfeld. Dieses birgt für Privatpersonen, Unternehmen und Behörden Herausforderungen und hierüber muss ständig neu verhandelt werden. Um hier sinnvolle Entscheidungen zu treffen, benötigen wir Wissen, dessen Vermittlung ein Grundanliegen unseres Hauses ist." Das Spektrum der behandelten Themen ist weit und reicht von rechtlichen Grundlagen über das Darknet sowie den Jugend- und Gesundheitsschutz über den Extremismus im Netz bis hin zum immer wieder aktuellen Thema Bildrechte. Zur Zeit ergeben sich ganz besonders aus der Corona-Pandemie und den damit einhergehenden Regelungen neue Fragestellungen zum Datenschutz, etwa was die Nutzung der Corona-Warn-App oder die Datenspeicherung der Luca App betrifft. Aber auch Distanzunterricht und mobiles Arbeiten von zuhause aus werfen Probleme auf, wenn es etwa um die Auswahl der verwendeten Video-Konferenzsysteme unter Datenschutzaspekten geht. Dass die nötige technische Infrastruktur für den Daten-Dienstag digital zur Verfügung steht, verdanken die drei Partner einerseits der Förderlinie „Neustart Kultur" der Bundesregierung und andererseits seit 2022 der DATEV Stiftung Zukunft, die das Projekt jetzt finanziell fördert. Tobias Meisel, Referent der Stiftung, begründet das Engagement so: „Die Interaktion mit Expertinnen und Experten aus dem Bereich des Datenschutzes in all seinen Facetten hat uns überzeugt den „DATEN-DIENSTAG-DIGITAL" in unserer neuen Förderpartnerrunde zu etablieren. Wir freuen uns sehr auf die Zusammenarbeit!"

Der Daten-Dienstag zeichnete sich von Anfang an durch eine gelungene Mischung aus einem Impulsvortrag und einer sich anschließenden angeregten Diskussion aus. Regelmäßig fanden 60 bis 120 Gäste aus der Region in das Museum in der Nürnberger Lessingstraße. Mit dem Umzug ins Digitale veränderte sich das Publikum. Die Teilnehmenden kommen aktuell aus dem gesamten deutschsprachigen Raum inklusive Österreich und der Schweiz. Via Chat können die Zuhörenden jederzeit Fragen stellen, ihre Meinung einbringen oder ergänzende Informationen teilen.

Das wird auch im Verlauf des Jahres 2022 hoffentlich so bleiben. Einen Aufriss aktueller Themen rund um die aktuelle EU-Datenschutz-Gesetzgebung bot der erste Vortrag anlässlich des Europäischen Datenschutztages. Ralf Bendrath, der als politischer Referent bei der Fraktion Die Grünen/ Europäische Freie Allianz tätig ist, benannte fünf aktuelle Themenbereiche. Dies sind der internationale Datenaustausch sowie die Kontrolle grenzüberschreitender digitaler Dienste und Märkte. Hinzu kommen Fragen zur Nutzung von künstlicher Intelligenz, zur Cybersicherheit oder zu terroristischen Inhalten im Netz. Schließlich stehen der Einsatz des Covid-19 Digitalzertifikats oder die eID, der Ausweis im Smartphone, auf der Agenda und geben sicher Anlass für weitere Daten-Dienstage.

Eine weitere Premiere feierte die Veranstaltungsreihe am Safer Internet Day, dem 8.2.2022, mit dem „Daten-Dienstag on Tour" aus dem Frankfurter Schwestermuseum für Kommunikation. Prof. Alexander Roßnagel, der hessische Datenschutzbeauftragte, sprach zum Thema: „Gemeinsam für ein besseres Internet. Herausforderungen aus der Sicht der Datenschutzaufsicht". Interessierte konnten entweder im Museum für Kommunikation Frankfurt dabei sein oder die Veranstaltung unter der Schirmherrschaft der hessischen Digitalministerin Prof. Kristina Sinemus via Zoom verfolgen und im Chat oder vor Ort mitdiskutieren. Prof. Roßnagel zeichnete die Entwicklung des Internets hin zu einem Ort allgegenwärtiger Datenverarbeitung, die Individuen nicht mehr kontrollieren können, nach.

Hier komme, so der Referent, dann dem Datenschutz die entscheidende Funktion zu für einen wirksamen Schutz- und Ordnungsrahmen zu sorgen. Um die Menge an Daten, die über den Einzelnen erfasst wird, möglichst gering zu halten, schlug er vor Datenschutzanwendungen bereits in die aktuell genutzten informationstechnischen Systeme zu integrieren. Das Netz und damit das Thema Datenschutz werden sich auch in Zukunft weiterentwickeln und so werden neue Herausforderungen entstehen.

Die Themen für den Daten-Dienstag werden nicht ausgehen. Dies beweist ein Blick in das weitere Programm des Jahres 2022: Hier werden unter anderem Themen wie „Hate Speech“, „Gesundheitsdaten“ oder „Kinderbilder im Netz“ behandelt; zudem wird die Veranstaltungsreihe im Schwestermuseum in Berlin zu Gast sein und das Jubiläum des 50. Daten-Dienstags im Juni sollte man sich auch schon einmal vormerken.

Weitere Informationen und die kommenden Themen finden sich auf der Website des Museums für Kommunikation Nürnberg unter https://www.mfk-nuernberg.de/datendienstag/

Hier können Interessierte auch einige der aufgezeichneten Vorträge nachschauen.

Über die Autorin

Dr. Vera Losse
leitet die Presse- und Öffentlichkeitsarbeit des Museums für Kommunikaton Nürnberg.

▶ https://www.mfk-nuernberg.de/

Museum für Kommunikation Nürnberg

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

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

DATENSCHUTZ-MOTIVE FÜR „DATENSCHUTZ GEHT ZUR SCHULE“ GESUCHT

David Heimburger

Noch bis Ende April läuft der Kreativwettbewerb der BvD-Initiative „Datenschutz geht zur Schule“ für Aufkleber zum Thema Datenschutz. Schüler:innen an allgemeinbildenden und weiterführenden Schulen sind aufgerufen Entwürfe für Klebe-Sticker einzusenden. Eine prominent besetzte Jury bestimmt die Gewinner:innen.

Wettbewerbsbeitrag von der 10-jährigen Cleo

Es ist immer das Gleiche: Zum Ende ihrer Vorträge ziehen die Dozent:innen der Initiative „Datenschutz geht zur Schule“ (DSgzS) ihr Ass aus dem Ärmel. Nach 90 Minuten oft lebhafter Diskussionen über Sicherheit bei Onlinediensten und den Schutz der eigenen Daten gibt es noch etwas zum Anfassen, Einstecken und Mitnehmen. Eine Karte mit den wichtigsten Tipps auf der einen und Webcam-Stickern auf der anderen Seite erfreuen sich als Give-away großer Beliebtheit.

Jetzt will DSgzS zusätzlich Aufkleber drucken lassen, die weiterhin die Sammelleidenschaft befriedigen und zugleich positive Botschaften zum Datenschutz in die Klassen- und Kinderzimmer transportieren. Aber was für Aufkleber gefallen der Zielgruppe? Keiner kann uns das besser sagen als die Schüler:innen selbst.

Daher hat DSgzS einen Kreativwettbewerb gestartet. **Bis 30. April** können Schüler:innen Entwürfe einschicken für Aufkleber, die „Ja“ zum Datenschutz sagen. Alles ist erlaubt, so lange die Botschaft eine positive ist und keine Urheberrechte Dritter verletzt werden.

Parallel soll der Wettbewerb dazu dienen, dass Lehrkräfte das Thema Datenschutz als Projektthema mit den Schüler:innen diskutieren können – zum Beispiel im Zusammenspiel mit den neuen Videos von DSgzS (siehe Seite 48). Entsprechend werden Preise für Klasseneinreichungen wie für Soloteilnehmende vergeben. Drei Klassen können jeweils 300 Euro Zuschuss zur Klassenkasse gewinnen, drei Einzelpersonen können je eine Sofortbildkamera und ein Set Kopfhörer gewinnen.

Eine prominente Jury aus Kreativen mit einem gutem Gespür für Jugendliche bestimmt die Sieger:innen. Der YouTuber **Morpheus** erklärt Informatik leicht verständlich. **Shary Reeves** ist TV-Moderatorin der Sendung „Wissen macht ah!“. **Steven Gätjen** moderiert unter anderem Sendungen mit Joko und Klaas. **Christine Links** stellt als TotallyGamerGirl Spiele vor. **Werner Fütterer** gehört zum Vorstand des Bunds der Kunsterziehenden.

Der Wettbewerb ist Anfang Januar gestartet. Der Aufruf zur Teilnahme wird sowohl über die Verteiler des BvD in die Datenschutzbranche kommuniziert wie über diverse Multiplikatoren aus dem schulischem Bereich.

Und: Jeder, der Kinder um sich hat, ist herzlich aufgerufen diese jetzt zur Teilnahme zu motivieren!

Alle Informationen zum Wettbewerb: www.bvdnet.de/kreativpreis

Über den Autor

David Heimburger
hat sich als Rechtsanwalt auf die Arbeit als Datenschutzbeauftragter spezialisiert. Der Hamburger prüft Geschäftsmodelle und unterstützt bei der Bereitstellung der erforderlichen Datenschutzdokumente. Seine Kunden sind kleine und mittlere Unternehmen sowie Vereine. Seine Schwerpunkte sind zum einen die Grundsatzberatung von Start-ups und zum anderen medizinische Einrichtungen wie Rettungsdienste und Arztpraxen.

▶ https://www.davidheimburger.de/

NEUE SERVICEANGEBOTE FÜR BVD-MITGLIEDER

Stephan Rehfeld

Der Bedarf an Software-Lösungen wird unter den Kollegen immer größer. Daher hat der BvD-Vorstand beschlossen, Mitglieder in Ihrer Arbeit zu unterstützen, indem er neue Projekte angestoßen hat, die Vorstandsmitglied Stephan Rehfeld an dieser Stelle kurz vorstellt.

Projekt 1: Software-Marktübersicht

Wer sich mit dem Thema Software auseinandersetzt, muss sich zunächst einen Überblick verschaffen, welche Angebote es auf dem Markt gibt. Dabei unterstützen wir unsere Mitglieder nun mit einer auf der Verbandswebsite verfügbaren Marktanalyse. Allerdings gibt es nicht die eine Lösung für alle Datenschutzprobleme. Daher haben wir die Software-Produkte in verschiedene Themenblöcke unterteilt.

Aktuell bearbeiten wir die folgenden Themen:

- Software zur Dokumentation des Datenschutzes (kurz Datenschutz-Software)
- Datenschutz-Managementsysteme
- Consent Management Plattformen
- Tools für Webseiten-Audits
- Generatoren für Datenschutzerklärungen
- eLearning-Lösungen

In einem ersten Schritt haben wir Software-Anbieter recherchiert und angeschrieben. Die Eintragungen beruhen also auf Selbstauskünften der Software-Anbieter. Allen Software-Anbietern wurde ein kostenloser Basiseintrag angeboten, damit für eine Listung keine Hürde aufgebaut wird.

Im Rahmen eines Premium-Eintrages ist es möglich, das eigene Produkt ausführlicher zu beschreiben. Zudem gibt es die Option, die Software-Lösung in einer ca. 30minütigen Videovorstellung zu präsentieren. Bei diesen Videopräsentationen steht im Vordergrund, dass sich Mitglieder einen Praxiseindruck von dem jeweiligen Produkt verschaffen können.

Wir freuen uns, wenn Sie das neue Tool des BvD nutzen und bitten Sie, uns fehlende Anbieter zu melden, damit wir die Listen ergänzen können.

Projekt 2: Von Nutzern für Nutzer – Erfahrungsaustausch über Software

Markttransparenz über die Anbieter von Software zu bekommen ist der erste Schritt für eine Software-Auswahl. Weiterhin wäre es aber sehr hilfreich, aus der Praxis zu erfahren, was die Vor- und Nachteile einzelner Software-Produkte sind. Daher entstand die Idee, dass Kollegen auf Regionalgruppentreffen von dem Praxiseinsatz von Produkten berichten. Dies soll ein reiner Erfahrungsaustausch sein und keine werbliche Vorstellung von Produkten. Daher haben wir aus diesem Projekt Software-Anbieter explizit ausgeschlossen.

Der BvD hat im Januar 2022 einen Aufruf unter den Mitgliedern gestartet, wer bereit ist, bei Treffen von Regionalgruppen von seinen eigenen Erfahrungen mit Software-Produkten zu berichten. Die Resonanz war sehr gut. Aktuell sind wir noch dabei, die Meldungen kommerzieller Anbieter zu diesem Projekt auszusortieren.

Mit erscheinen dieser BvD News sollte der „Referenten-Pool" dann bereinigt sein und für die Sprecher der Regionalgruppen zur Verfügung stehen. Diese können frei entscheiden, ob sie auf diesen Erfahrungsaustausch zurückgreifen wollen oder nicht.

Wir danken Michael Weimann für die Idee zu diesem Erfahrungsaustausch.

Über den Autor

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 im Leitungskreis des GDD-Erfa-Kreises Hannover engagiert, im AK Datenschutz der Bitkom und in der Fachgruppe Datenschutz von Niedersachsen. Digital e.V. 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.

MEINE AUFGABEN ALS DATENSCHUTZBEAUFTRAGTER

- Leitfaden für Verantwortliche in Unternehmen und Vereinen -

Rudi Kramer

Rudi Kramer
Meine Aufgabe als Datenschutzbeauftragter

C.H.Beck Verlag

1 Auflage 2022
56 Seiten
6,90 Euro
ISBN 978-3-406-74995-7

In Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat der Verlag C.H. Beck in der Reihe der Vorsorgebroschüren ein neues Heft mit dem Titel: „Meine Aufgaben als Datenschutzbeauftragter" veröffentlicht. Die Reihe der Vorsorgebroschüren, die fast durchgängig zu einem sehr verträglichen Preis von 6,90 € angeboten werden, richtet sich eher nicht an Spezialisten, sondern an Menschen, die an einem speziellen Thema Interesse haben und eine erste, gute Information dazu suchen. Vorgabe oder Empfehlung des Verlages ist es deshalb diese Broschüren in einer allgemein verständlichen Sprache zu schreiben und möglichst wenig Fachbegriffe zu verwenden und wenn diese dann in verständlicher Sprache zu erläutern.

Diese allgemeinen Rahmenbedingungen hat der Verfasser dieser Broschüre, Rudi Kramer, jahreslanges Mitglied im Vorstand des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. und Syndikusrechtsanwalt und Mitarbeitender in der Datenschutzabteilung eines der größten IT-Unternehmen Deutschlands, in hervorragender Art und Weise erfüllt.

Zielgruppe der Broschüre sind Mitarbeitende in Unternehmen (worunter hier nicht nur Industrie-Unternehmen, sondern auch Handwerksbetriebe, freiberuflich Tätige und Handelsunternehmen verstanden werden), die in ihrem Unternehmen zum Datenschutzbeauftragten benannt wurden oder benannt werden sollen oder sich um diese Aufgabe bewerben sowie Menschen, die die Dienstleistung des externen Datenschutzbeauftragten anbieten wollen.

Logisch richtig beginnt die Broschüre mit der Darstellung, wann ein Verantwortlicher – wie die oben genannten Unternehmen, die personenbezogene Daten verarbeiten, in der datenschutzrechtlichen Fachsprache genannt werden – einen Datenschutzbeauftragten benennen muss oder darf. Insofern wäre, worauf auch der Untertitel der Broschüre hinweist, die Zielgruppe um die Verantwortlichen in den Unternehmen zu erweitern, die sich darüber Klarheit verschaffen müssen, ob sie einen Datenschutzbeauftragten benötigen oder nicht.

Knapp die Hälfte der Broschüre befasst sich mit den Themen, wann ein Datenschutzbeauftragter bestellt werden muss oder kann, welche fachlichen Voraussetzungen er mitbringen muss und wie er zu benennen und wem gegenüber die Benennung mitzuteilen ist. Beim ersten Durchlesen der Broschüre erschien dieser Fragenkomplex überproportional viel Raum bekommen zu haben. Wenn man jedoch berücksichtigt, zu welchen Themen des Datenschutzbeauftragtendaseins Aufsichtsbehörden Stellung genommen haben oder auch Gerichtsverfahren anhängig gewesen sind, muss man sagen, dass diese Gewichtung praxisrelevant und zutreffend ist.

Die Broschüre kann von der Sprache und vom Umfang her ohne größere Probleme durchgelesen werden. Hilfreich sind dabei die hervorgehobenen Texte von besonderer Wichtigkeit und ebenso die erläuternden Hinweise. Die logisch richtige und sehr gute Gliederung ermöglicht es aber auch diese Broschüre als erstes Nachschlagewerk zu verwenden. Für die weitere Tätigkeit und Karriere als Datenschutzbeauftragter wird man nicht umhin kommen qualifizierte Kommentare und Veröffentlichungen der Aufsichtsbehörden zur Kenntnis zu nehmen, um seine Aufgabe als Datenschutzbeauftragter gut erfüllen zu können. Diesen Anspruch der Vermittlung vertiefender Erkenntnisse hat der Verfasser der Broschüre ausdrücklich nicht erhoben, sondern im Vorwort auf die Notwendigkeit der vertiefenden Befassung mit dem Thema Datenschutz verwiesen. Er hat dabei darauf hingewiesen, dass es sein Ziel sei Menschen in die Lage zu versetzen weitergehende Fragen zu stellen. Ob er dieses Ziel erreicht hat, kann nur sehr eingeschränkt vom Rezensenten beantwortet werden, weil er sich schon vielen weiterführenden Fragen hat stellen müssen. Diese Antwort müssen die hoffentlich zahlreichen Leserinnen und Leser der Broschüre sich selbst geben. Die Vermutung ist aber, dass der Autor sein Ziel erreichen wird.

Viele Menschen, die sich neu mit einem Themenkomplex befassen oder befassen müssen, wünschen sich Checklisten, um sich dann, wenn sie diese für sich positiv ausgefüllt haben, auf der sicheren Seite oder zumindest auf dem richtigen Weg zu fühlen. Diese Erwartung erfüllt der Verfasser mit einer Checkliste für Verantwortliche, um die Entscheidung für einen Datenschutzbeauftragten zu dokumentieren, und wohl noch relevanter mit einem detaillierten Beispiel von Fragestellungen im Rahmen eines Audits einer Videoüberwachungseinrichtung oder der Bestandsaufnahme für ein Schulungskonzept und insbesondere der Checkliste für „erste Tätigkeiten“ als Datenschutzbeauftragter. Die Übersichten und Checklisten zeigen die umfangreiche Erfahrung des Autors als Praktiker im Datenschutz und sind nicht nur als Hilfestellung für den Einstieg, sondern auch als Qualitätskontrolle für schon länger tätige Datenschutzbeauftragte gut geeignet. Wegen der leider auch im Datenschutz nicht irrelevanten Redensart: „Der Prophet im eigenen Land ist nichts wert.“ ist es für Datenschutzbeauftragte besonders wichtig sich mit anderen zu vernetzen und die Angebote der unterstützenden Organisationen, die Kapitel 7 ausführt, zu nutzen. Gerade interne Datenschutzbeauftragte, die in der Regel keinen Überblick darüber haben, wie andere Verantwortliche mit ähnlichen datenschutzrechtlichen Fragestellungen umgehen, können bei Annahme dieser Angebote für sich und für ihr Unternehmen enorm profitieren. Möglicherweise hat die Bescheidenheit des Verfassers ihn daran gehindert die hervorragenden Seminar- und Fortbildungsangebote des BvD deutlicher zu bewerben. Dies sei hiermit nachgeholt.

Eine leichte Kritik sei bezogen auf das Muster einer Benennung zum Datenschutzbeauftragten (intern) (S. 18) gestattet, soweit dort enthalten ist: Zusätzlich übernimmt der Datenschutzbeauftragte folgende Aufgaben: „Führen des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 Absatz 1 bzw. Abs. 2 DS-GVO“. Gerade wenn es darum geht einen Datenschutzbeauftragten neu in einem Unternehmen zu installieren, ist es wichtig deutlich auseinanderzuhalten, welche Aufgaben den Verantwortlichen und welche Aufgaben den Datenschutzbeauftragten betreffen. Es ist bekannt, dass in der Praxis sehr viele Datenschutzbeauftragte diese Verzeichnisse erstellen und pflegen. Wichtig wäre es aber darauf hinzuweisen, dass dies eine Aufgabe des Verantwortlichen ist. Diese verschafft ihm die Möglichkeit in seinem eigenen „Laden“ zu erkennen, wer in welchem Umfang mit personenbezogenen Daten arbeitet und wo deshalb datenschutzrechtliche Fragestellungen auftauchen, bei deren Lösung dann der Datenschutzbeauftragte helfen kann.

Nicht nur bei der vertiefenden Auseinandersetzung mit Datenschutzfragen, sondern auch bei der ersten Annäherung mit dem Thema können Informationen der Aufsichtsbehörden hilfreich sein. Insofern ist es sicherlich ein guter Service die Aufsichtsbehörden des Bundes und der Länder in der Broschüre zu nennen und Links auf deren Homepages aufzunehmen. Unglücklich ist in diesem Zusammenhang, dass die Links für die Aufsichtsbehörden in Bayern (BayLDA), Rheinland-Pfalz und Thüringen (S. 23) falsch sind. Dies mag insbesondere für den Verfasser und den Verlag ärgerlich sein, weil sie dies beim Korrekturlesen übersehen haben; problematisch ist es aber nicht, weil die richtigen Internetadressen ohne große Probleme von den Lesern auch selbst gefunden werden können.

Zusammengefasst ist festzuhalten, dass Rudi Kramer mit dieser Broschüre eine wertvolle Hilfestellung für alle, die sich erstmals mit der verantwortungsvollen Aufgabe eines Datenschutzbeauftragten auseinandersetzen, gelungen ist.

Rezension von

Thomas Kranig

war von 2011 bis 2020 Präsident des Bayerischen Landesamts für Datenschutzaufsich.

TTDSG LEICHT ERKLÄRT – EIN EINFACHER ÜBERBLICK ÜBER DAS NEUE TELEKOMMUNIKATIONS-TELEMEDIEN-DATENSCHUTZGESETZ

Jens Eckhardt

Viele haben noch gar nicht gemerkt, dass seit dem 1. Dezember 2021 für den Bereich der Telekommunikation und der Telemedien neue Regelungen gelten. An diesem Tag ist das TTDSG in Kraft getreten, das die Datenschutzbestimmungen aus der ePrivacy-Richtlinie (2002/58/EG) umsetzt und unter anderem die bisherigen Regeln aus dem Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG) in geänderter Form zusammenbringt. TTDSG ist die Abkürzung für Telekommunikations-Telemedien-Datenschutzgesetz, und das ist die Kurzform für „Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien".

Nochmal in Schlaglichtern verdeutlicht: Das TTDSG …

- … behandelt ein wichtiges Thema (ePrivacy umfasst alle elektronische Kommunikation),
- hat Relevanz für Unternehmen und Behörden sowie für fast jeden Lebensbereich (eben wie Internet und Telekommunikation) und
- zeigt offensichtliche Bezüge zu der DSGVO als zentrales Regelwerk für Datenschutz.

Daher gehört die Beschäftigung mit dem TTDSG quasi zum Pflichtprogramm einer/eines jeden Datenschutzbeauftragten.

In einer solchen Situation passiert in Deutschland typischerweise Folgendes: Mehrere etwa 1.000-seitige Kommentare werden vorangekündigt, die nach ein paar Monaten bis Jahren auf den Markt kommen. Auf jeder Datenschutzkonferenz widmen die Veranstalter dem TTDSG mindestens einen Vortragsslot für Übersichts- oder Spezialbeiträge; die bereitgestellten Präsentationen lassen einen großen Interpretationsspielraum. Die Aufsichtsbehörden beginnen mit der Aktualisierung des vorhandenen Materials. Und es wird viel diskutiert und gestritten, sodass die Liebhaber des Themas auf ihre Kosten kommen und jede Unzulänglichkeit des Gesetzes oder einer vertretenen Meinung genüsslich herauspräpariert wird – nur hilft dies in der Praxis nicht unbedingt weiter.

Das Buch „TTDSG leicht erklärt", das zu den ersten Veröffentlichungen über das TTDSG gehört, verfolgt einen anderen Ansatz: Der Autor Dr. Jens Eckhardt nimmt seine Lesen:innen mit auf eine Reise durch das TTDSG. Die Grundstrukturen werden zu Beginn in gebotener Ausführlichkeit erklärt: welches Verhältnis zum ePrivacy-Recht auf EU-Ebene besteht, wie sich der Vorrang der DSGVO auswirkt und wie sich Telekommunikation und Telemedien voneinander abgrenzen lassen. Anschließend folgt der Mini-Kommentar der Struktur des TTDSG und behandelt die einzelnen Vorschriften. „Mini" bedeutet hier aber nicht „wenig informativ": Im Gegenteil, keine Regelung kommt zu kurz, und stets ergänzen Hinweise aus relevanten Materialien – beispielsweise aus Orientierungshilfen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) – den Text zu den spezifischen Themen. Nie verliert der Autor sein Publikum aus dem Blick: das sind vor allem Rechtsanwender:innen, Datenschutzbeauftragte und sonstige ePrivacy-Praktiker:innen. Wer keine juristische Vorbildung hat, aber bereit ist sich auf die juristische Materie einzulassen, wird behutsam an die Regelungen herangeführt.

Jens Eckhardt
TTDSG leicht erklärt – Ein einfacher Überblick über das neue Telekommunikations-Telemedien-Datenschutzgesetz

PrivacyExpert

1. Auflage 2021
96 Seiten
85,55 Euro

Der Normtext wird nicht einfach wiederholt, sondern derart aufbereitet, dass die (im Gesetzestext manchmal zugegeberweise etwas versteckte) Logik für alle Lesenden deutlich wird.

Dies schlägt sich auch in der Darstellungsform nieder: kurze Textteile, viele gliedernde Zwischenüberschriften, Zusammenfassungen der Abschnitte, Kästen mit Praxistipps, Übersichten in Tabellen und viele erklärende Schaubilder, die in einem stimmigen Layout zum Verständnis beitragen. Insgesamt hat der Autor die zumindest von vielen Nicht-Jurist:innen als trocken empfundene juristische Materie so textlich und visuell aufbereitet, dass sich mehr Menschen davon angesprochen fühlen und den Stoff aufnehmen können. Das zeichnet das Buch aus. So strengt das Lesen der knapp 100 Seiten trotz des komplexen Themas nicht an. Auch muss man das handliche Buch nicht von vorn bis hinten studieren, sondern findet die Antworten zu den eigenen Fragen relativ schnell, sobald man erkannt hat, ob der Sachverhalt zur Telekommunikation oder zu den Telemedien zuzurechnen ist.

Für Neulinge, die mit dem TTDSG arbeiten müssen oder wollen, ist der Text ein passabler Einstieg ins Thema ePrivacy, weil sie an die Hand genommen und mit Beispielen, Daumenregeln oder Tipps unterstützt werden. Doch auch für diejenigen, die schon lange im Geschäft sind, lohnt sich die Lektüre: Wer sich nicht bereits selbst über beide Ohren ins TTDSG gestürzt hat und ohnehin mit der gesamten Materie tiefgreifend vertraut ist, wird vermutlich Neues lernen.

Die Tabelle mit der Zuordnung zwischen den Regelungen im TKG a. F. ist hilfreich für diejenigen, die ihre auf der alten Rechtslage beruhenden Texte wie Verfahrensbeschreibungen, Sicherheitskonzepte, Datenschutzerklärungen oder sonstige Handreichungen mit Informationspflichten anpassen müssen, nutzbringend sind auch jene Abschnitte, in denen inhaltliche Änderungen zwischen alter und neuer Rechtslage hervorgehoben werden. Betont wird außerdem, dass sich die Regelungen des TTDSG – wie auch die europäischen ePrivacy-Vorgaben – nicht nur auf Datenschutzfragen, also die Verarbeitung von Daten natürlicher Personen, beziehen, sondern dass der Anwendungsbereich größer ist.

Die (zu dem Zeitpunkt der Drucklegung noch aktuelle) Positionierung der deutschen Datenschutzaufsichtsbehörden für Anbieter von Telemedien aus dem Jahr 2019 stellt der Autor dar, macht aber auch deutlich, welche der Argumentationslinien aus seiner anwaltlichen Sicht nicht zwingend und welche alternativen Ansätze denkbar sind. Offene Rechtsfragen benennt er als solche, die bisherige Rechtsprechung sowie Leitlinien des Europäischen Datenschutzausschusses und Materialien einiger Aufsichtsbehörden in anderen Mitgliedstaaten greift er auf. Man merkt Dr. Jens Eckhardt – Fachanwalt für IT-Recht – an, dass er weiß, wovon er spricht. Sein Fokus liegt auf der Rechtsanwendung in der Praxis und Vermittlung des notwendigen juristischen Know-hows, um die Rechtskonformität von ePrivacy-Sachverhalten prüfen und bewerten zu können.

In dem sich entwickelnden und von hoher Dynamik geprägten Rechtsgebiet – man denke nur an aufsichtsbehördliche und gerichtliche Entscheidungen in Deutschland und Europa, die ab Anfang 2022 bekannt geworden sind – zeichnet sich ab, dass die informative Zusammenstellung „TTDSG leicht erklärt“ eine baldige Aktualisierung verdient. In diesem Zuge würden gewiss nicht nur die an das TTDSG angepassten Orientierungshilfe der DSK und die neue Rechtsprechung Berücksichtigung finden, sondern es könnten auch Stellen, an denen sich – vermutlich der Veröffentlichungshektik geschuldet – Tippfehler oder Doppelungen eingeschlichen haben, verbessert werden. Wünschenswert für eine Folgeauflage wäre ein Index der wichtigen Begriffe, um bei Praxisfragen direkt in die relevanten Textstellen hineinspringen zu können.

Im Vorwort verspricht Dr. Jens Eckhardt einen einfachen Überblick über das neue TTDSG, eine Einordnung der Regelungen in den Kontext der rechtlichen und tatsächlichen Rahmenbedingungen und eine erste Orientierung „gerade auch für Unstimmigkeiten und Unklarheiten des TTDSG“. Diese Ankündigung erfüllt er auch, jedenfalls so gut wie nur möglich. Vor allem das letzte Versprechen – die erste Orientierung angesichts einer eben doch weiterhin nicht vollständig klaren Rechtslage und einzelner Widersprüche im Gesetzestext selbst – löst er ein. Dies ist ein echter Mehrwert in der Debatte, besonders weil der Autor die vorhandenen Unstimmigkeiten nicht kaschiert und es trotzdem schafft, die Lesenden in dieser unsicheren Situation nicht völlig im Dunkeln zu lassen. Steht dies nicht im Widerspruch zum versprochenen „einfachen Überblick über das TTDSG“? Nein. Hier passt ein Albert Einstein zuschriebenes Zitat: „Mache die Dinge so einfach wie möglich. Aber nicht einfacher.“ In diesem Sinne handelt es sich bei dem Buch „TDDSG leicht erklärt“ keineswegs um eine übermäßig simplifizierte oder gar banale Ausarbeitung, sondern um eine ansprechend aufbereitete und für die Praxis taugliche Arbeitshilfe rund um das TTDSG für Rechtsanwender:innen und Datenschutzbeauftragte.

Rezension von

Marit Hansen

Die Informatikerin ist Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD).

DATENSCHUTZ IM UNTERNEHMEN

Michael Wächter

Michael Wächter
Datenschutz im Unternehmen

C.H.Beck Verlag

6. Auflage 2021
492 Seiten
79,00 Euro
ISBN: 978-3-40675402-9

Bereits die 5. Auflage war 2018 Gegenstand einer Rezension. Nach wie vor profitiert das Werk von der Praxisnähe des Autors, der als Unternehmensjurist tätig ist. Bereits an den Überschriften lässt er erkennen, dass die Zielgruppe an rechtlichen Themen außerhalb des Datenschutzrechts interessiert sein sollte. Gleichwohl ist dieses Werk auch dem Datenschutzbeauftragten zu empfehlen, der sich strukturiert anhand von Themengebieten mit Rechtsmaterien vertraut machen will.

Die Kapitel untergliedern sich in „Datenschutz im Unternehmen", „Datenschutzkontrolle", „Pflichten des Unternehmens", „IT-Sicherheit in Unternehmen", „Rechte der Betroffenen", „Externe Datenverarbeitung" und „Haftung im Datenschutzrecht".
Die Darstellung des Datenschutzes als Unternehmensaufgabe wird im ersten Kapitel ausführlich dargestellt. Bestehende Missverständnisse, „das sei ja alles nur Aufgabe des Datenschutzbeauftragten" werden dadurch bereits zu Anfang widerlegt. Die DSGVO als Regelungsvorgabe wird gut nachvollziehbar zu anderen rechtlichen Themengebieten dargestellt. Im Rahmen der IT-Nutzung im Arbeitsverhältnis werden die Fragen zum Beschäftigtendatenschutz behandelt.

Die Ausführungen zum Datenschutz bei der Nutzung von Telemedien erleiden, soweit es

sich nicht um die allgemeinen und historischen Darstellungen handelt, das Schicksal, das durch das zwischenzeitlich in Kraft getretene TTDSG die rechtlichen Grundlagen durch den Gesetzgeber geändert wurden.

Im Kapitel zur Datenschutzkontrolle stehen wie bereits in der vorherigen Auflage erfreulicherweise nicht nur der betriebliche Datenschutzbeauftragte und die Aufsichtsbehörde im Fokus, sondern auch die Selbstkontrolle, das Verzeichnis der Verarbeitungstätigkeit und die Mitbestimmung. Bei den Pflichten der verantwortlichen Stelle werden die Anforderungen an die Rechtmäßigkeit der Verarbeitung und Übermittlung sowie die damit verbundenen Transparenzpflichten beschrieben. Hervorzuheben ist, dass sich der Autor hier in einem Abschnitt ausführlich der Kybernetik und dem maschinellen Lernen widmet und in diesem Bereich auch ein Prüfschema für die Zulässigkeit des Einsatzes von künstlicher Intelligenz unter den Aspekten der Rechtmäßigkeitsgrundlagen von Art. 6 Abs. 1 lit. b und lit. f DS-GVO bietet.

Ausführlich werden im Kapitel zur IT-Sicherheit technische, aber auch organisatorische Maßnahmen und diese nicht nur zur IT, sondern auch zu allen Informationen dargestellt. Hinweise zur Klassifikation können praxisnah übernommen werden. Den Rechten der betroffenen Person wird ein eigenes Kapitel gewidmet, ebenso dem Sachverhalt „Externen Datenverarbeitung".

Der Blick des Praktikers im Unternehmen wird im abschließenden Kapitel zur Haftung im Datenschutzrecht erkennbar, wenn hier neben der Haftung bei Verletzung der Privatsphäre auch Fragestellungen zu wettbewerbs- und urheberrechtlichen Verstößen, der Arbeitnehmerhaftung, Verstöße gegen Diskriminierungsverbote und bei Internetkriminalität angesprochen werden. Auch hier wurde die Betrachtung um die technische Entwicklung fortgeführt, wenn sich der Autor auch mit Ausführungen zu den Fragestellungen zur Haftung und Unterlassen bei Algorithmen befasst. Den Abschluss bilden wie bisher Ausführungen zu versicherungsrechtlichen Fragen.

Immer wieder werden in diesem Werk Einzelthemen vertieft, Begrifflichkeiten erläutert und Musterformulierungen dargestellt. Erfreulicherweise wurde zudem die Anzahl an Mustertexten und Checklisten zur Vorauflage erhöht.

Keinen Anspruch erhebt das Werk darauf einen Kommentar zu ersetzen. Sein Vorteil liegt auch in der 6. Auflage darin zentral einen fundierten Überblick über die zu beachtenden Fragestellungen zu verschaffen, die neben dem originären Datenschutzrecht in angrenzenden Rechtsgebieten bei der Beratung von Unternehmen aufkommen können. Und es belässt es nicht nur bei den Fragestellungen, sondern bietet auch Lösungsansätze an. Unglücklich erscheint der Veröffentlichungszeitpunkt kurz vor Ende einer Legislaturperiode des nationalen Gesetzgebers, der in dieser Zeit dann noch Änderungen durchführte, die nun unberücksichtigt bleiben mussten wie im BetrVG oder eben die Einführung des TTDSG.

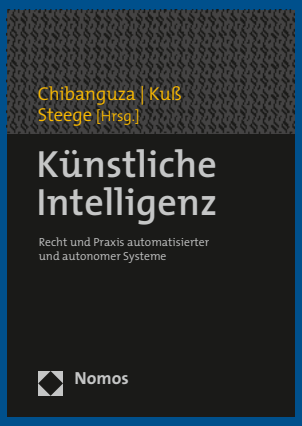
Im Ergebnis bleibt es trotz dieser kleinen Einschränkung ein leicht lesbares Fachbuch, das nicht nur für das Management eines Unternehmens gut geeignet ist sich mit den relevanten Fragestellungen vertraut zu machen. Es bietet (nicht nur) dem betrieblichen Datenschutzbeauftragten wertvolle Argumentationshilfen in der Beratung zu den aktuellen Fragestellungen.

Rezensionen von

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

KÜNSTLICHE INTELLIGENZ - RECHT UND PRAXIS AUTOMATISIERTER UND AUTONOMER SYSTEME

Dr. Kuuya Josef Chibanguza, Christian Kuß, Hans Steege (Hrsg.)



Dieses Praxishandbuch ist kein Lehrbuch, das den Einstieg in die komplexe Materie der künstlichen Intelligenz (KI) ermöglichen soll. Vielmehr handelt es sich um ein wissenschaftlichen Ansprüchen gerecht werdendes Werk für Fortgeschrittene, dessen Herausgeber damit eine für Praxis und Wissenschaft zugleich kompakte Gesamtdarstellung der Materie geben wollen. Im Lichte dessen ist zunächst erstaunlich, dass es keinen einleitenden Teil mit Begriffserklärungen, Definitionsversuchen und historischen Abhandlungen gibt, die mit Blick auf die teils inflationäre Benutzung des Akronyms „KI" oder der Bonmots Algorithmus und „Machine Learning" aufräumen. Geschuldet ist dies vermeintlich der Erwartungshaltung der Herausgeber, dass die Leserschaft dieses Grundlagenwissen mitbringt. Zumindest wird diese Annahme durch den vorangestellten Grundlagenteil bekräftigt. Dort nimmt Kultusstaatsminister a.D. Julian Nida-Rümelin einen überraschend anderen, unerwarteten philosophischen Einstieg in die Materie, der sich mit Gründen für Handlungen auseinandersetzt und raffiniert die Brücke vom menschlichen zum computergestützten Auslösen von Handlungen schlägt.

Im Allgemeinen zeichnet sich das Werk durch eine sehr breite, namhafte Autorenschaft mit herausragender Expertise aus. Neben zu erwartenden Vertretern der Jurisprudenz sind auch zahlreiche andere Fakultäten wie die Arbeitspsychologie, Ethik, Informatik, Ingenieurwissenschaften, Sozialwissenschaften, Theologie sowie Verkehrs- und Wirtschaftswissenschaften vertreten. Sie bringen insbesondere für die sektorspezifischen Darstellungen im zweiten Teil des Handbuchs (zu Verkehr/Mobilität, Medizin, Produktion/Handel, HR, Finanzen, Justiz/Anwaltschaft, Polizei/Militär, Verwaltung, Medien/Suchmaschinen/Uploadfilter/soziale Medien/Social Bots) ein großes Spektrum an fachlichem Spezialwissen ein. Dementsprechend geht das Handbuch weit über datenschutzrechtliche und -spezifische Fragestellungen und Themen hinaus ohne den Nutzen des Handbuchs für Datenschutzberater zu schmälern. Dies hängt insbesondere mit dem sehr ordentlichen und zweckdienlichen Stichwortverzeichnis zusammen, das die Tauglichkeit als Nachschlagewerk begründet und Schlagworte sehr gut recherchieren lässt. Die Abhandlungen zum Datenschutz der Herausgeber Christian Kuß und Hans Steege setzen sich detailliert mit Fragen des räumlichen und sachlichen Anwendungsbereichs, der verantwortlichen Person sowie der Rechtsgrundlagen, Datenschutzgrundsätze und Rechte der Betroffenen nebst Profiling auseinander. Datenschutzberater finden dort umfangreiche fachliche Hilfestellung für die im Zusammenhang mit der Nutzung von KI einhergehenden Herausforderungen beispielsweise im Bereich der Datenschutzfolgen-Abschätzung und von Privacy by Design. Besonders erwähnenswert sind diesbezüglich auch die Ausführungen des Berliner Rechtsprofessors Carsten Momsen im 1. Teil (§ 2 G. 18 ff.) zu den Zusammenhängen von Big-Data-Analysen und KI. Überzeugend stellt er den besonderen Wert der Errungenschaft von Big-Data-Analysen für KI dar, der sich argumentativ auch für den Datenschutz mit Blick auf Datensicherheit fruchtbar machen lässt. Denn ebenso wie die Kriminalistik kommt die Datensicherheit nach dem Stand der Technik ohne engmaschige Analyse von Maschinendaten nicht aus, um ausgefeilte Cyberangriffe zuverlässig abwehren zu können.

Zusammenfassend lässt sich das Handbuch dementsprechend uneingeschränkt für Datenschutzberater empfehlen, die sich regelmäßig tiefgehend mit KI und seinen zahlreichen Facetten im digitalen Alltag auseinanderzusetzen haben. Für sie hält das Handbuch zahlreiche Handlungshilfen, Lösungsvorschläge und Inspiration bereit, die sich sehr gut in Bewertungen und Stellungnahmen integrieren oder transformieren lassen.

Dr. Kuuya Josef Chibanguza, Christian Kuß, Hans Steege (Hrsg.)
Künstliche Intelligenz - Recht und Praxis automatisierter und autonomer Systeme

Nomos Verlagsgesellschaft

1. Auflage 2022
1.350 Seiten
158,00 Euro
ISBN 978-3-8487-7161-5

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
07.04.2022	**Webinar** – Orientierungshilfe Telemedien 2021 der DSK
08.04.2022	**Webinar** – Aktuelle Urteile und Entscheidungen
12.04.2022	**Präsenzseminar** – Datenschutzaudit und Datenschutzkontrolle in Frankfurt/Main
29.04.2022	**Webinar** – Bezahlen mit Daten – kein Kopplungsverstoß mehr!
09.05.2022	**Sonderseminar** – Dokumentationspflichten des Datenschutzbeauftragten in Berlin
09.05.2022	**Sonderseminar** – Beschäftigtendatenschutz in Berlin
09.05.2022	**Sonderseminar** – Die Einführung von Microsoft 365 in Berlin
10. - 11.05.2022	**BvD-Verbandstage 2022**
08.06.2022	**Online-Seminar** – Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)
28.06.2022	**1. Datenschutztag Hessen & Rheinland-Pfalz für behördliche, kommunale und betriebliche Datenschutzbeauftragte**

Zeitsparend Fachwissen erhalten nach Artikel 37, Absatz 5 DSGVO

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

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

Die wichtigsten Daten der BvD-Gremien

Die Arbeitskreise und Regionalgruppen sind wichtige Gremien innerhalb des BvD. Detaillierte Informationen zu den Treffen und den Terminen finden Sie unter:

▶ www.bvdnet.de/regionalgruppen
▶ www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

28.04.2022	RG Nord	**20.05.2022**	AK Externe
05.05.2022	RG Gütersloh	**24.05.2022**	RG West
16.05.2022	AK Sozial	**24.06.2022**	RG München
16.05.2022	RG Ost	**30.06.2022**	RG Nord

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-Knowhow 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
Leiter des BvD-Hauptstadtbüros
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 e.V. 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 2021
Preisverleihung 12. Mai 2022 auf den BvD-Verbandstagen in Berlin.
DAME 2021

Schulprojekt

Datenschutz geht zur Schule BvD e.V. DATENSCHUTZ GESTALTEN

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

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

privacy4people POWERED BY BvD

privacy4people - Gesellschaft zur Förderung des Datenschutzes gGmbH

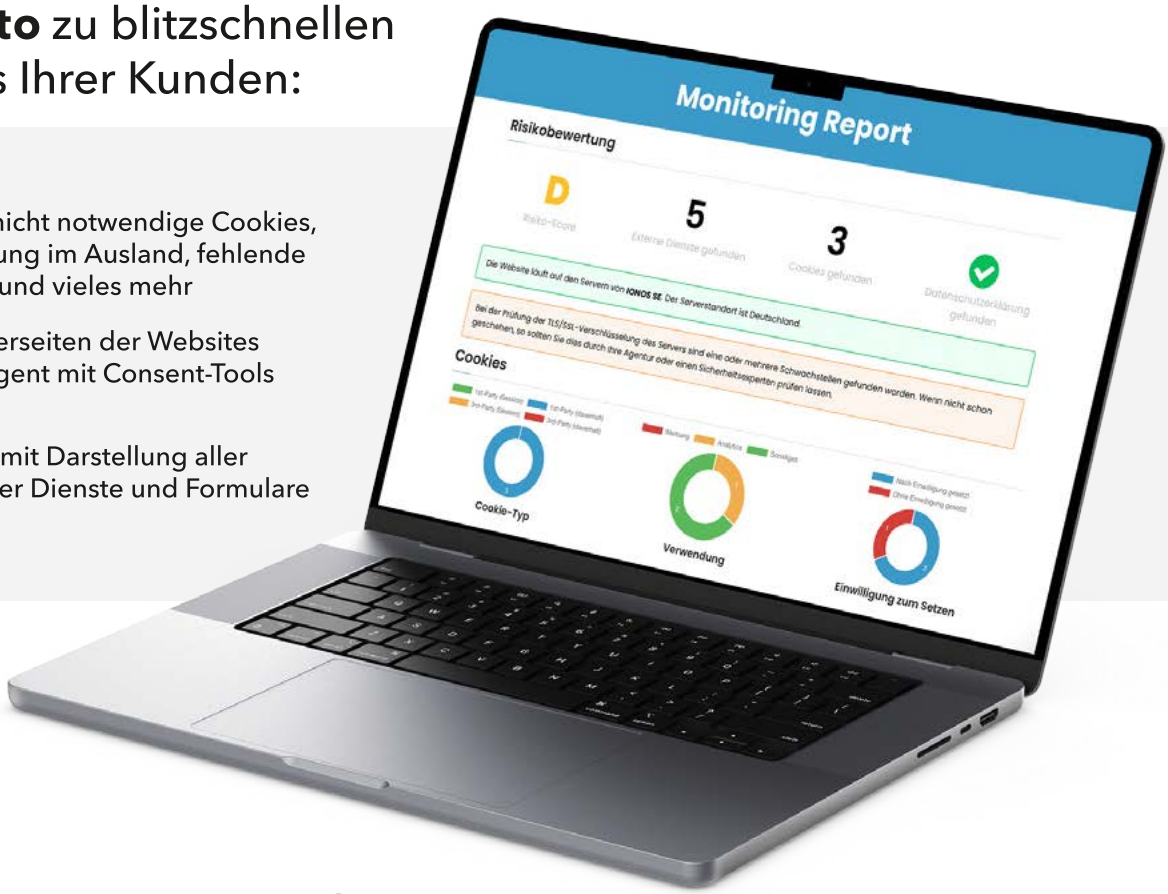
IHRE SPENDE FÜR DEN DATENSCHUTZ:
Commerzbank
IBAN: DE 30 5054 0028 0424 5577 00
BIC: COBADEFFXXX

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

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**.