Ausgabe 03/2022

BvD-NEWS

Fachmagazin für Datenschutzbeauftragte

Seite 42

DIGITALISIERUNG DER SCHULEN UND MEDIENKOMPETENZ – WO KLEMMT'S

TLfDI Dr. Lutz Hasse, René Rösel

Seite 12

„DIE CHATKONTROLLE WIRD VOR GERICHT LANDEN."

Interview mit EU-Abgeordnetem Patrick Breyer

Seite 6

DER DATA ACT IN DER KRITIK

BvD, Stiftung Datenschutz und DIHK luden zur Diskussion mit Fachleuten nach Berlin

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

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

BvD e.V.
DATENSCHUTZ GESTALTEN

Der Frühjahrskongress der Datenschutz-Community

2023

BvD-Verbandstage

09.05. – 10.05.2023

IM DORINT HOTEL
KURFÜRSTENDAMM BERLIN

KÖNNEN WIR UNS DATENSCHUTZ NOCH LEISTEN?

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

SPANNENDE VORTRÄGE MIT NAMHAFTEN REFERENT:INNEN

- Prof. Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Carl Fabian Lüpke (Flüpke), Chaos Computer Club (CCC)
- Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen
- Carmen Wegge, MdB (SPD)
- Prof. Dr. Heribert Prantl, Süddeutsche Zeitung

Im Rahmen der BvD-Verbandstage findet am Abend des 09.05.2023 die Verleihung des Datenschutz Medienpreises DAME 2022 statt. Seien Sie mit dabei!

TEILNAHMEGEBÜHREN:

Frühbucherrabatt bis 8. Februar 2023
BvD-Mitglieder & Behörden: 795 €
Nichtmitglieder: 1.050 €

Ab dem 9. Februar 2023
BvD-Mitglieder & Behörden: 895 €
Nichtmitglieder: 1.150 €

Alle Preise zzgl. gesetz. MwSt.

JETZT ANMELDEN:
www.bvdnet.de/bvd-verbandstag

BvD e.V.
DATENSCHUTZ GESTALTEN

Liebe Leserinnen und Leser,

„DSGVO im 5. Jahr – Wie hat die EU den Datenschutz verändert?" – so war die sechste BvD-Herbstkonferenz überschrieben, die wir Ende Oktober gemeinsam mit den Datenschutzaufsichtsbehörden aus Baden-Württemberg und Bayern veranstaltet haben. Wenn man diese Frage in aller Kürze beantworten wollen würde, müsste man wohl sagen: von Grund auf. Das sorgte selbst in Deutschland, wo wir – verglichen mit manch anderem europäischen Partner – über viele Jahrzehnte Erfahrung im Datenschutz verfügen, zunächst für einige Anlaufschwierigkeiten. Seitdem hat sich zum Glück einiges getan.

Unser Kongressmotto darf aber nicht darüber hinwegtäuschen, dass es längst weitere Gesetzesvorhaben aus Brüssel gibt, die den Datenschutz teilweise massiv berühren. In zügigem Tempo kommen neben der DSGVO neue Rechtsvorschriften wie der Digital Services Act oder bald der Data Act oder der AI Act hinzu, die wir als Datenschutzbeauftragte zukünftig kennen und in ihrem Verhältnis zur DSGVO verstehen müssen. Der Grundgedanke dieser Gesetzesvorhaben in Europa ist eigentlich gut. Im Data Act beispielsweise geht es um das Teilen von Daten, darum, innovative digitale Geschäftsmodelle in Europa zu fördern. Es geht um Effizienzgewinne, Umweltschutz, Energieeinsparung. Aber funktioniert das auch? Das Problem ist hier, dass diejenigen, für die diese Rechtsakte eigentlich gedacht sind, in den entsprechenden Gesprächen in Brüssel nicht oder erst zu spät mit am Tisch sitzen. Das bestätigte bei der Herbstkonferenz auch Renate Nikolay, Kabinettschefin von EU-Kommissions-Vizepräsidentin Věra Jourová. Die großen Digitalkonzerne sind an diesen Diskussionen seit Jahren beteiligt, während die Perspektive der deutschen Wirtschaft unterrepräsentiert ist in der EU. Für diese Problematik gilt es zu sensibilisieren.

Die Vielzahl der neuen digitalpolitischen Rechtsakte bedeutet für uns Datenschutzbeauftragte aber auch: Die Anforderungen an die Beratungen werden stets umfangreicher und es gilt am Ball zu bleiben, um Verantwortliche bei einer praktikablen Umsetzung datenschutzkonformer Geschäftsprozesse kompetent zu begleiten. Beginnen können Sie damit gleich in dieser Ausgabe der BvD-News, die einen Schwerpunkt auf europäische Themen setzt – so etwa mit dem Nachbericht zu unserem Informationstag zum Data Act (S. 6) oder dem Interview mit dem EU-Parlamentarier Dr. Patrick Breyer von der Piratenpartei. Oder Sie lesen, was Steffen Kroschwald über die Gestaltung nutzer-, kontext- und situationsadäquater Verarbeitungsumgebungen vor dem Hintergrund des Artikel 25 DSGVO und des AI Act schreibt.

Europäische Gesetzgebung macht einiges oft komplizierter, manchmal aber auch einfacher. Vor wenigen Tagen ist es uns nach vielen Jahren (Überzeugungs-)Arbeit gelungen eine Genehmigung der baden-württembergischen Aufsichtsbehörde für die von BvD und GDD gemeinsam entwickelte Verhaltensregel „Trusted Data Processor" zu erhalten, die wesentliche Datenschutzprozesse der Auftragsverarbeitung konkretisiert. Sie verfolgt das Ziel durch Prozessstandardisierung die Umsetzung von Datenschutzanforderungen zu vereinfachen und transparenter zu machen sowie die Beauftragung von geeigneten Auftragsverarbeitern zu erleichtern. Vor allem erhöht die aufsichtsbehördliche Genehmigung der Verhaltensregel letztlich für die Beteiligten die Rechtssicherheit.

Mit einer Selbstverpflichtung auf die Verhaltensregel „Trusted Data Processor" machen Auftragsverarbeiter nach außen sichtbar, dass sie den in der Verhaltensregel festgelegten Vorgaben folgen und sich deren Überwachung durch eine Kontrollstelle unterwerfen. Im Falle von „Trusted Data Processor" ist dies die DSZ - Datenschutz Zertifizierungsgesellschaft mbH. Sie hat unter www.verhaltensregel.eu eine Website eingerichtet, auf der die Verhaltensregel zur Verfügung gestellt wird, so dass Sie die mit detaillierten Mustern gespickte Verhaltensregel als ein Hilfsmittel für Ihre tägliche Arbeit nutzen können – unabhängig davon, ob Sie sich der Verhaltensregel offiziell unterwerfen oder nicht. Falls Sie für Ihre Kunden oder Ihren Arbeitgeber mehr über die Verhaltensregel und deren Implementierung erfahren möchten: Der BvD bietet zu dem Thema kostenlose Informationsveranstaltungen sowie detailliertere Webinare und Seminare an. Informieren Sie sich einfach auf unserer Website oder fragen Sie in unserer Geschäftsstelle an.

Doch nun wünsche ich Ihnen erst einmal eine anregende Lektüre Ihrer BvD-News.

Ihr

Thomas Spaeing
BvD-Vorstandsvorsitzender

INHALTSVERZEICHNIS

IM FOKUS

Der Data Act in der Kritik
BvD, Stiftung Datenschutz und DIHK luden zur Diskussion mit Fachleuten nach Berlin.
Ulrich Hottelet 6

„Die Chatkontrolle wird vor Gericht landen."
EU-Parlamentarier Patrick Breyer (Piratenpartei) spricht im Interview mit den BvD-News über die geplante Chatkontrolle und die weiteren Digitalisierungsvorhaben der EU.
Patrick Breyer 12

Synthetische Daten und Datenschutz – eine Momentaufnahme
Das Berliner Unternehmen Statice entwickelte eine Technologie, die der Finanz-, Versicherungs- und Gesundheitsbranche synthetische Daten zur Verfügung stellen will.
Omar Ali Fdal 14

DATENSCHUTZRECHT

Nutzer-, kontext- und situationsadäquate Verarbeitung by Design
Wie dies vor dem Hintergrund von Art. 25 DSGVO und KI-Verordnung gelingen kann zeigt
Prof. Dr. Steffen Kroschwald 18

Das Recht auf Auskunft in der Datenschutz-Grundverordnung – Art. 15 DSGVO
Pseudonyme Informationen gelten nach DSGVO als personenbezogene Daten. Ausgenommen sind anonyme Informationen, die keiner Person zugeordnet werden können.
Nicole Schmidt, Elif Tüysüz 23

DATENSCHUTZPRAXIS

Cybersicherheit in der „VUKA-Welt"
Cyberangriffe gehören zum Alltag von Unternehmen. Was nach einem Angriff zu tun ist erläutert der Präsident der Cyber-Sicherheitsagentur Baden-Württemberg
Ralf Rosanowski 28

DANE als Lösung für sichere E-Mail-Übertragung
Wie sich technisch DANE als Konfiguration von E-Mail-Verschlüsselung umsetzen lässt erläutern
Leo Dessani und Prof. Dr. Ronald Petrlic 33

Datenhandel im Spannungsfeld von DSGVO, DGA und DA
Manche Unternehmen wollen Daten kommerziell nutzen. Wie dies rechtskonform gelingen kann erläutert
Dr. Kristina Schreiber 38

IMPRESSUM:
BvD-News
Das Fachmagazin des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

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

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

Fotos (sofern nicht anderweitig ausgewiesen):
Fotos: 123RF, Adobe Stock,
Fotos Data-Act-Tagung von BvD, Stiftung Datenschutz und DIHK: Andreas Burkhardt
Fotos BvD-Herbstkonferenz und Behördentag: Uli Schneider

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.

AUFSICHTSBEHÖRDEN

(Thüringer) Schulen: Digitalisierung und Medienkompetenz – wo klemmt's?
Die Digitalisierung von Schulen kommt nur zögerlich voran. Woran das liegt analysiert Thüringens Datenschutzbeauftragter
Dr. Lutz Hasse und Co-Autor Renè Rösel 42

Social Media und öffentliche Stellen:
Was ist beim Betrieb einer Fanpage zu beachten?
Viele Behörden und Verwaltungen betreiben Facebook-Fanpages. Sie müssen aber auch die Rechtmäßigkeit der Datenverarbeitung gewährleisten, erläutert
Johanna Krieger 50

50 Jahre Datenschutz in Hessen
Der Hessische Datenschutzbeauftragte erinnerte mit dem 25. Wiesbadener Forum Datenschutz an das erste Datenschutzgesetz.
Maria Christina Rost 52

GESELLSCHAFT

Wie KI vertrauenswürdig wird
Datenschutz erhöht die Akzeptanz für künstliche Intelligenz - ist das Zentrum für vertrauenswürdige KI überzeugt.
Philipp Otto, Verena Till 54

AUS DEM VERBAND

Was kommt aus Brüssel und Washington auf die DSB zu?
Die Digitalvorhaben aus Brüssel beschäftigen auch die BvD-Herbstkonferenz und den Behördentag in Stuttgart. Die BvD-News dokumentiert drei zentrale Vorträge zu Data Act, AI Regulations und dem geplanten neuen Privacy Shield mit den USA.
Christina Denz 58

Vom Bonner Tulpenfeld zum Hochschul-Campus in Ulm
Die Geschichte des BvD spiegelt die Geschichte der Datenschutzbeauftragten und ihrer Anerkennung als Beruf.
Prof. Dr. Gerhard Kongehl, Dr. Bernd Beier 62

Kurz gefasst
Mitgliederversammlung beschließt einstimmig neue Satzung 64
Weiterbildung für die Lebenswelt von Kindern und Jugendlichen 65
Kunst für den LfDI 66
Linkttipps 67
Endspurt zur DAME 2022 67

REZENSIONEN

Future Law 68
Datenschutz und Data Science 69
IT-Sicherheit 70
Mach das Internet aus, ich muss telefonieren 71
Überblick Rezensionen 2022 72

TERMINE / SERVICE

Termine der Regionalgruppen und Arbeitskreise des BvD 74

ULRICH HOTTELET

DER DATA ACT IN DER KRITIK

BvD, Stiftung Datenschutz und DIHK luden zur Diskussion mit Fachleuten nach Berlin

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V., der Deutsche Industrie- und Handelskammertag (DIHK) und die Stiftung Datenschutz haben mit ihrer gemeinsamen Veranstaltung „Data Act: Was kommt auf die Wirtschaft zu?" am 5. September in Berlin die Datenschutzaspekte des Gesetzes beleuchtet. Zahlreiche Sprecherinnen und Sprecher verschiedener staatlicher und wirtschaftlicher Organisationen nahmen dazu Stellung.

Professor Dr. Stephan Wernicke, Chefjustitiar des DIHK, erinnerte zum Auftakt der Veranstaltung an das ambitionierte und die Interpretation leitende Ziel der EU-Datenstrategie: „Die EU soll an die Spitze einer datengetriebenen Gesellschaft und Wirtschaft gebracht werden", sagte er. Die vier im Rahmen der EU-Digitalstrategie geplanten Gesetzeswerke sorgten in der Datenwirtschaft aber für reichlich Diskussionsstoff. Dabei den Überblick zu behalten sei auch für Experten herausfordernd. „Es ist verwirrend, denn wir haben selbst für Juristen eine solche Anzahl von unterschiedlichen Regelungen, dass man immer wieder erstaunt sein kann", räumte der Europarechtsprofessor ein und skizzierte die Zwecke des Data Acts: „Ziel ist ein gemeinsamer rechtlicher Rahmen für das Nutzen und Teilen von Daten. Entlang der Wertschöpfungskette sollen Daten besser genutzt werden beziehungsweise die Nutzung erst ermöglicht werden. Kurz: Es geht also um das faire Teilen." Ein Großteil der Wirtschaft sei betroffen und noch nicht ausreichend sensibilisiert. Dabei werde der Data Act die bisherige Praxis, wie Daten genutzt und geteilt werden, tiefgreifend verändern. Damit betreffe er die Geschäftsmodelle vieler Unternehmen, betonte Wernicke.

Der Entwurf beschreibe das Verhältnis zur Datenschutz-Grundverordnung (DSGVO) in knappen Worten: „Die Regulierungen der DSGVO bleiben unberührt vom Data Act." Wernicke hält das für unzureichend. „Wir müssen Lehren ziehen aus den Schwierigkeiten der Anwendung der DSGVO", betonte er. „Lassen Sie uns gemeinsam Wege finden den Gesetzestext noch zu verbessern. Wir werden uns insbesondere dafür einsetzen, dass die Anliegen der KMU vertreten werden und dass Rechtssicherheit, Rechtsklarheit und Praxistauglichkeit gewahrt werden mit diesem Entwurf." Andernfalls würde der Data Act Innovationsfähigkeit behindern, wie sich zum Beispiel bei den intelligenten digitalen Stromzählern, den Smart Metern, zeige: „Wie gehen wir damit um? Sind es personengebundene oder maschinelle Daten? Lassen sie sich verbinden? Wir wissen, dass Datenschutzbeauftragte von Fachaufsichtsbehörden und Finanzämtern diese Frage unterschiedlich behandeln." Wernicke forderte Klarheit, ob und wie die DSGVO Anwendung finde. Gerade nach den Erfahrungen mit der DSGVO müsse Rechtssicherheit zwingend bereits im Gesetzestext hergestellt werden und nicht erst durch sich über viele Jahre hinziehende Auslegungen der Aufsichtsbehörden oder Gerichtsentscheidungen.

Dr. Christoph Bausewein

Klare Gesetze gefordert

Dr. Christoph Bausewein, Rechtsanwalt und Vorstandsmitglied des BvD, betonte, wie wichtig die Verständlichkeit des Verordnungstexts sei: „Wir brauchen anwendbare, auslegbare Gesetze, die nicht, wie wir es in der DSGVO erleben, von den Aufsichtsbehörden ausgelegt werden müssen, sondern wo sich die Rechtsanwender zurechtfinden." Des Weiteren sei es wie bei den anderen großen digitalen Regulierungen wichtig Zielkonflikte zu vermeiden. „Jetzt ist noch das Bekenntnis da, dass die DSGVO uneingeschränkt gelten und den Maßstab bilden soll. Schwierig wird es für Datenschutzbeauftragte, wenn es um die Auslegung geht. Was ist dann von der Datenverarbeitung noch zulässig?"

DIE DEUTSCHE WIRTSCHAFT BRAUCHT EINE STARKE STIMME IN BRÜSSEL!

Thomas Spaeing

Im Rahmen eines Privacy-Club-Termines, den der BvD im Frühjahr 2022 veranstaltet hat, kam das Thema der neuen EU-Acts erstmals umfassend zur Sprache. Ein Rechtsanwalt mit tieferen Einblicken in die Verhandlungen in Brüssel stellte damals den derzeitigen Gesprächsstand der Verhandlungen dar. Bei der aus Vertretern verschiender Verbände und Institutionen bestehenden Runde führte dies zu Diskussionen.

Wie es aussah und inzwischen bestätigt ist, wurde in Brüssel unter Mitwirkung der US-Digitallobby über die kommenden Regelungen verhandelt. Die deutsche Wirtschaft und insbesondere der deutsche Mittelstand waren nicht vertreten. Hier werden die Regelungen aber massive Auswirkungen haben.

Die Diskussion in der exklusiven Runde führte dazu, dass der BvD eine eigene Veranstaltung zu diesem Thema vorschlug. Die Stiftung Datenschutz und auch der DIHK waren sofort bereit daran mitzuwirken und auch Ressourcen bereitzustellen. So konnte innerhalb weniger Wochen das Konzept für die Veranstaltung am 05.09.2022 entwickelt und unter tatkräftiger Mitwirkung aller Beteiligten erfolgreich umgesetzt werden.

Dabei geht es in dieser Phase der Verhandlungen nicht in erster Linie um den Datenschutzbeauftragten, sondern darum, dass für die deutsche Wirtschaft ggf. erhebliche Nachteile und langfristig negative Auswirkungen zu erwarten sind, wenn diese nicht ebenfalls mit starker Stimme an den Verhandlungen in Brüssel beteiligt ist. Die Digitalkonzerne verfolgen hier ganz eigene Ziele für künftige Geschäftsmodelle. Die europäischen Unternehmen kommen darin erst als Datenspender und dann als Kunden vor.

Es ist vollkommen unrealistisch zu erwarten, dass alle Unternehmen gleichermaßen von den dann meist zwingend zu teilenden Daten profitieren werden. Um die Daten auswerten und deren Potential monetarisieren zu können, sind unter anderem erhebliche Fachkompetenz und IT-Systeme in einem Maße erforderlich, wie sie zumindest im Mittelstand nicht vorhanden sind. Wenn in Deutschland zurzeit über 100.000 Fachkräfte allein in der IT-Sicherheit fehlen, dann bekommt man eine Ahnung, dass Experten zur Betreuung komplexer Datenmodelle und Modellierungen für die nächsten zehn Jahre ebenfalls fehlen werden. Es entwickelt sich also eine Abhängigkeit, die für den Wirtschaftsstandort Deutschland fatal werden kann. Hier ist die Politik, aber auch die Wirtschaft gefordert sich massiv einzubringen. Befragungen bei Unternehmern zu diesem Thema haben gezeigt, dass diese die Digitalisierung ihrer Prozesse eher einschränken würden, als ihre sensiblen Prozessdaten und Geschäftsgeheimnisse aller Welt zur Verfügung zu stellen.

Es geht hier um die elementaren Daten der jeweiligen Geschäftsmodelle, also das hart erarbeitete Know-how der deutschen Industrie. Dieses zu schützen bedeutet auch den Wirtschaftsstandort zu schützen. Und dies gilt tatsächlich für ganz Europa: Warum sollten die Unternehmen der EU sich solchen einseitigen, nachteiligen Regelungen unterwerfen und ihr Know-how kostenlos zu Markte tragen? Natürlich würden andere weltweit davon profitieren, aber hier gehen Wirtschaftskraft und Arbeitsplätze verloren. Wir werden uns weiter für die Beteiligung in Brüssel und für bessere sinnvolle Regelungen einsetzen. Unterstützen Sie das und sensibilisieren Sie Ihre Unternehmen für das Thema.

Benjamin Brake

In die gleiche Richtung argumentierte **Benjamin Brake**, Leiter der neu geschaffenen Abteilung "Digital- und Datenpolitik" im Bundesministerium für Digitales und Verkehr. Der Data Act liege mit den politischen Prioritäten der Bundesregierung und insbesondere des Digitalministeriums auf einer Linie, nämlich mehr und bessere Daten zur Verfügung zu stellen. „Wir begrüßen grundsätzlich die Zielrichtung des Data Act. Aber der Teufel liegt im Detail", sagte Brake, forderte aber: „Wir wollen eine konsequente Trennung von DSGVO und Data Act sehen. Wir wollen nicht, dass datenschutzrechtliche Fragen in den Data Act hineingetragen werden, und wir wollen schon gar nicht eine Verschärfung der datenschutzrechtlichen Regeln auf europäischer Ebene. Ich weiß, das ist deutlich einfacher gesagt als getan."

Als zweite wichtige Frage nannte Brake den Umgang mit dem Thema Business to Government, das heißt unter welchen Bedingungen Unternehmen Daten dem Staat oder auf staatliche Nachfrage zur Verfügung stellen müssen. „Was wir nicht möchten, ist eine übermäßige bürokratische Belastung der Unternehmen. Und wenn die Regelungen so kommen, wie sie momentan diskutiert werden, nämlich dass sowohl der Anlass unklar ist als auch die Frage, welche Daten gemeint sind bei Business to Government, dann ist das eine Unklarheit, die für Unternehmen relativ schwer ist, insbesondere wenn es

darum geht sich auf den Datentransfer vorzubereiten." Brake sprach sich für eine Einschränkung aus. Entweder müsse klar sein, welche Daten Unternehmen vorhalten müssten für staatliche Zwecke und Anfragen oder man müsse das stärker eingrenzen. „Beides wird eine Herausforderung bei den Verhandlungen in Brüssel", prognostizierte der Vertreter des Digitalministeriums.

EU-Kommission hofft auf baldigen Kompromisstext im Rat der EU

Anna Ludin, Policy Officer für die Generaldirektion Kommunikationsnetze, Inhalte und Technologien der EU-Kommission, wirkte am Entwurf mit. Angestrebt werde „die faire Allokation von Wertschöpfungen in der Datenökonomie", betonte sie. Deshalb gehe es im Data Act auch um Datenzugangsverpflichtungen. Sie hofft, dass noch im Dezember ein Kompromisstext vorliegen und das Europäische Parlament im Februar über ein erstes Verhandlungsmandat abstimmen werde. Ludin erläuterte: „Wenn man sich die Kommissionsmitteilungen aus den Jahren 2014 und 2017 näher anschaut, dann gibt es eine gewisse Kontinuität vom Ansatz in Bezug auf die Datenökonomie. Man will eigentlich keine neuen Exklusivitätsrechte etablieren, sondern mehr Akteure befähigen, an der Wertschöpfung teilzuhaben und das durch Zugangsrechte. Das tut der Data Act im IoT."

Anna Ludin

Christian Dürschmied, Rechtsanwalt der Wirtschaftskanzlei Eversheds Sutherland und Policy Consultant für Datenschutz & Privacy beim Bundesverband Digitale Wirtschaft (BVDW) wies auf die wirtschaftliche und innovative Bedeutung von Daten hin, die der gesamten Gesellschaft nutzten. Gleichzeitig müsse ein hohes Maß an Vertrauen, Schutz und Sicherheit gewahrt werden. Übergeordnetes Ziel sei es Europa zum weltweit führenden Akteur in der Datenwirtschaft zu machen, indem ein „echter Binnenmarkt für Daten" geschaffen werde.

Er zeigte sich zugleich überzeugt, dass viele Unternehmen im Grundsatz zunächst den Data Act unterstützten. Sie schätzten die Innovations- und Investitionsanreize für digitale Geschäftsmodelle sowie die Markt- und Wettbewerbschancen, sähen aber auch die technischen Herausforderungen und rechtliche Risiken durch drohende Sanktionen bei Verstößen. Es sei zudem für viele eine Herausforderung festzustellen, ob ihre Produkte und Verarbeitungstätigkeiten in den Anwendungsbereich des Data Act fallen.

DATA ACT: HINTERGRUND UND ZIELE

- Daten sind zentraler Bestandteil der digitalen Wirtschaft und wesentliche Ressource für die Sicherung des ökologischen und digitalen Wandels („Datennutzen allen")
- Volle Ausschöpfung des Potenzials datengesteuerter Innovationen, u. a. durch Möglichkeiten der Weiterverwendung von Daten und Abbau von Hemmnissen
- Hohes Maß an Vertrauen, Schutz, Sicherheit: Wahrung hoher Datenschutz- und Sicherheitsstandards, Schutz von vertraulichen Geschäftsdaten und Geschäftsgeheimnissen, Einschränkung von Datenzugriffen aus Drittstaaten
- Echter Binnenmarkt für Daten, Europa als weltweit führender Akteur in der datenagilen Wirtschaft
- Erleichterter Datenzugang und erleichterte Datennutzung sektorübergreifend
- Anreize für Investitionen in die Wertschöpfung durch Daten
- Stärkung der Innovationsfreundlichkeit und -fähigkeit
- Wettbewerb und faires Geschäftsumfeld (Abbau von Marktungleichgewichten, z.B. aus Datenkonzentration, Wettbewerbsbeschränkungen, Marktzutrittsbeschränkungen, Beeinträchtigungen von Datenzugang und Datennutzung, Ungleichgewichte bei Fachwissen und Verhandlungspositionen)
- Handlungskompetenzen des Einzelnen wirksam stärken
- Handlungsmöglichkeiten bei außergewöhnlicher Notwendigkeit wie öffentlichen Notständen
- Interoperabilitätsrahmen

Quelle: Christian Dürschmied

Die Konferenz wurde live über die Website https://data-act.org/ gestreamt. Dort können Interessierte Videos der einzelnen Beiträge weiterhin abrufen.

Unterschiedliche Interessenlagen in den Unternehmen

Im Interview mit **Frederick Richter**, Vorstand der Stiftung Datenschutz, erläuterte **Dirk Binding**, Leiter des Bereichs Digitale Wirtschaft und Infrastruktur bei der DIHK, die Herausforderung für die rund 3,4 Millionen IHK-Unternehmen in Deutschland. „Wir haben Unternehmerinnen und Unternehmer, die Daten herstellen. Wir haben aber auch welche, die die Daten nutzen, und dann haben wir andere Unternehmen, die die Daten gerne nutzen würden, aber im Moment noch nicht nutzen können. Es gibt also sehr unterschiedliche Interessen, die es zusammenzuführen gilt." Eine Befragung der Mitgliedsunternehmen erbrachte als deren großes Problem die Unsicherheit. „Wie kann ich Daten verwenden? Wie kann ich Daten weitergeben? Und wie kann der andere sie nutzen? Vielen Unternehmerinnen und Unternehmern sind die Folgen

Frederick Richter

Dirk Binding

des Data Act noch nicht bewusst. Wir müssen das so übersetzen, dass unsere Unternehmen es verstehen und keine Angst davor haben", sagte der DIHK-Vertreter. Bei deren Sensibilisierung stehe man noch am Anfang.

Dr. Vera Demary, Leiterin des Kompetenzfelds Digitalisierung, Strukturwandel und Wettbewerb im Institut der Deutschen Wirtschaft (IW), veröffentlichte kürzlich die Studie „Der Data Act. Welchen Rahmen Unternehmen für Data Sharing wirklich brauchen". „Unsere Erkenntnis ist: Unternehmen brauchen den Data Act so noch nicht. Denn die Unternehmen sind einfach noch nicht so weit." Nach einer IW-Befragung von Unternehmen aus Industrie und industrienahen Dienstleistungen im Jahr 2021 sind nur 29 Prozent von ihnen in der Lage Daten effizient zu bewirtschaften. Gründe dafür seien Rechtsunsicherheit und mangelnde Informationen über die Rechtslage. Lediglich elf Prozent könnten Daten effizient

bewirtschaften und austauschen. Der Großteil der Unternehmen gebe keine eigenen Daten heraus, sondern nehme Daten von Dritten in die eigenen Prozesse auf. „Es müssen unternehmensintern noch viele Dinge geklärt und organisiert werden. Und deswegen glaube ich, es ist noch nicht der richtige Zeitpunkt für den Data Act“, sagte Demary.

MÖGLICHE ANSATZPUNKTE FÜR EINEN KOMPROMISS

Dr. Vera Demary, vom Institut der Deutschen Wirtschaft (IW) formuliert vier Bereiche, die der Data Act beantworten muss:

1. Klärung des Anwendungsbereichs

Welche Daten sind gemeint (Rohdaten oder weiterverarbeitete Daten)? Welche Unternehmen sind gemeint? Ist die Schwelle von 50 Mitarbeitern geeignet?

2. Klärung der Rollen

Wer ist Dateninhaber, wer ist Nutzer? Wertschöpfungsketten und -netzwerke sind komplex. Andere Konstellationen würden KMU vieles leichter machen.

3. Verbesserung der Sicherheit

Wie lassen sich Geschäftsgeheimnisse besser schützen? Wie wird das überprüft?

4. Klärung der Begleitung

Wie werden Compliance und Wirkung des Data Act geprüft? Sind die Effekte gewünscht? Fördern sie größere Datenökonomie und bessere Datennutzung?

*Quelle: **Dr. Vera Demary,** Leiterin des Kompetenzfelds Digitalisierung, Strukturwandel und Wettbewerb im Institut der Deutschen Wirtschaft*

In der Diskussion zum Thema „Welche Rahmen brauchen Unternehmen für das Data Sharing?“ kritisierte **Klemens Gutmann**, Gründer und Vorsitzender des Unternehmens regiocom, dass die EU-Kommission mit dem Data Act einen „riesigen Universalhut“ schaffen wolle, statt sich drei bis fünf kleinere Hüte für die jeweilige Situation zuzulegen. Bei der DSGVO lag der der Vereinheitlichungsansatz auf der Hand. Es sei um Personen, um Einzelrechte in 27 Mitgliedstaaten

Dr. Vera Demary

gegangen. Beim Data Act aber gebe es unterschiedliche Anforderungen, Anwendungsbereiche und Risiken. Die kenne die Wirtschaft und auch der Gesetzgeber zum Teil noch nicht. In der Wirtschaft unterschieden sich zudem die Positionen zum Data Act je nach Branche. Während es zum Beispiel bei Daten aus der Flugzeugindustrie häufig um Geschäftsgeheimnisse gehe, sei das bei Verbrauchsdaten in der Energiewirtschaft ganz anders. Daher sei er skeptisch, ob es überhaupt eine gemeinsame legislative Lösung für die verschiedenen Anforderungen geben könne.

Mike Gahn, geschäftsführender Gesellschafter der ownSoft, kritisierte unter anderem die geplante Regelung, dass Unternehmen ab 50 Mitarbeitende und einem Jahresumsatz von mehr als zehn Millionen Euro vernetze Produkte und Services so gestalten sollen, dass die generierten Daten den Nutzenden direkt und leicht zugänglich sind. „Ich glaube nicht, dass ich ansatzweise geschützt bin durch die 50-Mitarbeiter-Klausel, weil unsere Kunden größer sind und mit den Anforderungen, die im Gesetz formuliert sind, konfrontiert sind.“ Er gehe davon aus, dass sich dadurch auch kleinere Firmen wie ownSoft an die Vorgaben halten müssen. „Das tickert bis ganz nach unten durch. Ich habe keine Chance mich dem zu entziehen.“

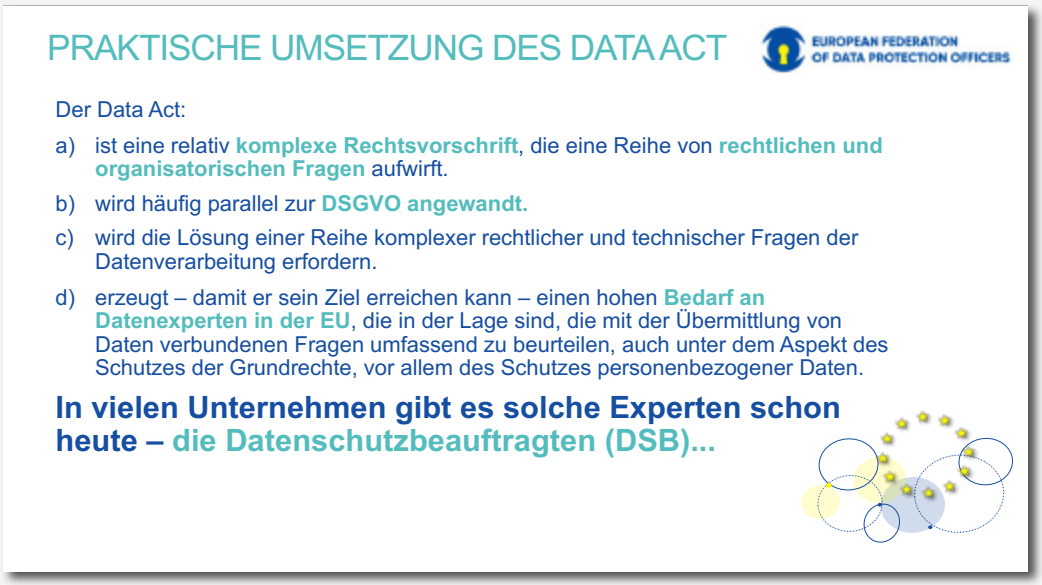
Thomas Fuchs

EU-Datenregulierungen sind nicht aufeinander abgestimmt

Thomas Fuchs, der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, sieht im Data Act, dem Data Governance Act und der DSGVO ein „mittelalterliches Triptychon, also drei Tafelbilder, die nebeneinander stehen und drei verschiedene Geschichten erzählen. Und das ist nicht richtig gut“. Da die DSGVO Rechtsgrundlage für die Übermittlung personenbezogener Daten sei, müsse nach DSGVO-Standards ermittelt werden. Das Einwilligungsmodell sei jedoch für eine auf eine massenhafte Datenteilung angelegte Wirtschaft nicht sinnvoll. „Das wird nicht funktionieren“, kritisierte Fuchs. Beim Data Act gebe es keinen europäischen Koordinierungsmechanismus wie bei den anderen Datenrechtsakten. „Ich weiß nicht, wie man das in der Praxis behandeln soll. Das Einzige, was es halbwegs kohärent machen kann, ist, dass die Datenschutzaufsichtsbehörden auch zuständig werden für die Koordination des Data Acts, weil nur sie im Data Act als *competent authorities* genannt werden.“

Vladan Rámiš, Vizepräsident des europäischen Dachverbands der betrieblichen Datenschutzbeauftragten, der European Federation of Data Protection Officers (EFDPO), sieht den Data Act eher als Konzentration auf die Perspektive des einzelnen Nutzers, nicht auf die des Teilens von Datenbanken, die für Big Data eigentlich notwendig seien. Er sprach sich zugleich für eine starke Rolle der Datenschutzbeauftragten in der Umsetzung aus: „Wie oft sind die Datenschutzbeauftragten im Data Act und in der gemeinsamen Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten zum Data Act erwähnt? Leider kein einziges Mal. Dennoch werden die Datenschutzbeauftragten häufig beteiligt sein an der Umsetzung des Data Act, weil sie sehr eng mit der DSGVO zusammenhängt.“

Am Ende der Diskussion zog Fuchs ein Fazit: „Viele Stellungnahmen heute gingen in dieselbe Richtung: Der Ansatz ist zu breit, die Begriffe sind zu unpräzise, die Abgrenzung zur DSGVO funktioniert nicht. Eigentlich müsste man sich fragen: Warum muss es ein Act sein? Ist es nicht ein typischer Fall für eine Richtlinie, wo der nationale Gesetzgeber sektorenscharf konkretisieren kann?“



Quelle: JUDr. Vladan Rámiš, Ph.D.

Der BvD veröffentlichte gemeinsam mit der Stiftung Datenschutz und dem DIHK ein Positionspapier zum Data Act. Über den QR-Code gelangen Sie zur Website der Veranstaltung:

Positionspapier von BvD, Stiftung Datenschutz und DIHK zum geplanten Data Act:

Entwurf der EU-Kommission zum Data Act als jpg-Download:

Über den Autor

Ulrich Hottelet
ist freier Journalist mit den Themenschwerpunkten Datenschutz, IT-Sicherheit und Künstliche Intelligenz.

Foto: Oliver Franke

"DIE CHATKONTROLLE WIRD VOR GERICHT LANDEN."

Der EU-Parlamentarier Patrick Breyer (Piratenpartei) sprach mit den BvD-News über die geplante Chatkontrolle, deren Auswirkungen auf Unternehmen und Behörden sowie über den aktuellen Stand der weiteren EU-Vorhaben zur Digitalisierung.

BvD-News: *Herr Breyer, die Chatkontrolle beschäftigt die EU-Kommission und das EU-Parlament bereits seit Längerem. Wie ist der aktuelle Stand?*

Patrick Breyer: Im ersten Schritt hat die EU den Anbietern von E-Mail-, Messaging- und Chatdiensten erlaubt private Nachrichten nach verdächtigen Inhalten zu durchsuchen, das machen bisher wohl nur US-Dienste wie GMail, Facebook Messenger und Microsofts X-Box. Im nächsten Schritt soll die Chatkontrolle jetzt für sämtliche Anbieter verpflichtend angeordnet werden. Das ist so, wie wenn die Post alle Briefe öffnen und scannen würde – völlig inakzeptabel. Dieser Verordnungsentwurf wird im europäischen Rat gerade mit Hochdruck beraten, allerdings hinter verschlossenen Türen. Das EU-Parlament berät parallel. Weil der Druck hoch ist, rechne ich damit, dass die Verordnung nächstes Jahr schon verabschiedet werden kann.

BvD-News: *Wie soll nach den bisherigen Plänen die Verordnung zur Chatkontrolle nach Inkrafttreten in den jeweiligen EU-Mitgliedsstaaten umgesetzt werden?*

Patrick Breyer: Die Verordnung selbst soll ohne Umsetzung unmittelbar gelten. In allen EU-Ländern soll eine Behörde Anbieter zur Chatkontrolle verpflichten können, wenn ein Dienst zum Versand illegaler Darstellungen oder zur Kontaktaufnahme zu Minderjährigen missbraucht werden kann. Das Problem ist, dass alle Kommunikationsdienste dafür missbraucht werden könnten, es sei denn, die Anbieter würden Minderjährige von ihren Diensten ausschließen. Dazu aber wiederum würden alle Nutzer, also auch Erwachsene, zur Altersverifizierung ihre Identität offenlegen müssen. Damit würde die Chance auf anonyme Kommunikation etwa für Journalisten, Whistleblower oder politische Aktivisten zerstört – davon abgesehen, dass selbst alle 17-Jährigen die meisten Apps nicht mehr installieren könnten. Das alles ist inakzeptabel.

BvD-News: *Wie hoch schätzen Sie die Möglichkeit ein, über die Chatkontrolle tatsächlich Kinderporno-Ringen auf die Spur zu kommen?*

Patrick Breyer: Solche Straftäter und Gruppen sind im Dark Web aktiv und setzen dort eigene Dienste und Foren auf. Und das werden sie auch weiterhin tun. Solche Gruppen sind nicht auf Facebook oder Whatsapp unterwegs. Und das bedeutet: Die eigentlichen Straftäter können weiterhin anonym chatten, aber die normalen Bürgerinnen und Bürger, die sich technisch nicht so auskennen, werden durchleuchtet und womöglich zu Unrecht verdächtigt. Solche Fälle gab es ja schon. Nach Angaben der Schweizer Bundespolizei sind 80 Prozent der automatisiert angezeigten Kommunikation strafrechtlich nicht relevant.

Und dennoch werden die Strafverfolger mit maschinellen Anzeigen überflutet und haben dadurch weniger Kapazitäten gezielt nach Kinderporno-Ringen im Netz zu fahnden. Und damit schadet die Chatkontrolle mehr dem Schutz der Kinder, als dass sie nützt. Davon abgesehen, dass in aller Regel die Ermittler auf die Spur solcher Ringe durch gezielte Hinweise kommen – und nicht zufällig durch die Durchleuchtung millionenfacher Daten.

BvD-News: *Der Datenschutz spielt dabei offenbar keine Rolle mehr.*

Patrick Breyer: Er taucht nur noch als Lippenbekenntnis auf, dass die Chatkontrolle unter Wahrung des Datenschutzes durchgeführt werden solle. Aber der Europäische Gerichtshof hat bereits 2020 gegen Frankreich entschieden, dass eine anlasslose Auswertung privater Kommunikation das Grundrecht auf Privatsphäre verletzt und nur ausnahmsweise bei Bedrohung der nationalen Sicherheit gerechtfertigt sei, nicht als Dauermaßnahme. Es liegen bereits Rechtsgutachten vor, die die Chatkontrolle als grundrechtswidrig bewerten. Sie könnte allenfalls dann verhältnismäßig sein, wenn sie gegen Tatverdächtige angeordnet wird. Sie darf aber nicht gegen die gesamte Bevölkerung gerichtet werden. Wenn die Verordnung kommt, wird sie vor Gericht landen. Ich selbst habe ja im Mai bereits eine Unterlassungsklage gegen Meta als Mutterkonzern von Facebook vor dem Amtsgericht Kiel gegen die verdachtslose automatisierte Durchsuchung privater Chatverläufe und Fotos eingereicht. Allerdings dürfte eine Entscheidung noch eine Weile dauern.

BvD-News: *Welche Auswirkungen hätte die Chatkontrolle auf in der Cloud gespeicherten Daten?*

Patrick Breyer: Auch die Cloud müsste durchleuchtet werden. Dort werden ja auch viele Fotos gespeichert, auch private, die nie geteilt werden. Gerade für Unternehmen und Behörden wird es ein Dilemma sein, ob sie weiterhin elektronische Kommunikationsdienste nutzen und darüber womöglich sensible Daten austauschen oder in der Cloud speichern sollten. Zudem dürfte die Fehlerquote der Algorithmen, die dort zum Einsatz kommen, sehr hoch sein. Software zur Suche nach Anbahnungsversuchen wurde etwa auf Englisch entwickelt, wie kann sie in anderen Sprachen funktionieren? Außerdem veröffentlichen die Unternehmen die Algorithmen nicht. Wir wissen also nicht, welche Kriterien zu welcher Durchleuchtung führen. Das müssen Datenschutzbeauftragte, die Behörden oder Unternehmen beraten, auf alle Fälle berücksichtigen.

BvD-News: *Es könnte also nur noch eine Ende-zu-Ende-Verschlüsselung helfen?*

Patrick Breyer: In Ende-zu-Ende-verschlüsselte Messenger soll eine Hintertür eingebaut werden. Wenn der Nutzer selbst verschlüsselt, könnte die Kommunikation nicht durchleuchtet werden. Das kann für eine Dateiablage funktionieren. Aber bei der Kommunikation per Mail beispielsweise unterstützen die wenigsten Empfänger eine Ende-zu-Ende-Verschlüsselung. Das ist übrigens auch noch die Herausforderung beim Digital Markets Act. Der ermöglicht ja die plattformübergreifende Nutzung von Messenger-Diensten. Dann müssen aber alle kompatible Verschlüsselung entwickeln.

BvD-News: *Wie bewerten Sie den Digital Services Act?*

Patrick Breyer: Auch hier konnten wir ein Gebot der Verschlüsselung nicht durchsetzen, auch kein Verbot der Vorratsdatenspeicherung. Stattdessen können künftig auch in Deutschland Konten und Veröffentlichungen gelöscht werden, wenn es fragwürdige Gesetze in Ungarn und Polen bereits ermöglichen. Das macht Zensur möglich. Das als Digitales Grundgesetz geplante Vorhaben verdient den Namen nicht. Es gibt leider die Tendenz in der EU der Wirtschaft und den Staatsorganen die Nutzung von Daten weitestgehend zu ermöglichen.

BvD-News: *Und wie sehen Sie die Verhandlungen zu den AI Regulations?*

Patrick Breyer: Die EU hat ein Forschungsprojekt finanziert, das herausfinden sollte, ob sich per Video-Analyse erkennen ließe, ob EU-Einreisewillige bei der Einreise wahre oder falsche Angaben machen. Das war natürlich wissenschaftlich nicht haltbar. Meine Hoffnung ist, dass im geplanten KI-Gesetz weder Forschung noch die Technologie selbst bei solcherart unethischen und unrechtmäßigen Fragestellungen zugelassen wird. Wir werden sehen, wie die Beratungen weiterlaufen. Zurzeit berät der europäische Rat über die Vorschläge der EU-Kommission. Das EU-Parlament will sich bis Jahresende zum Entwurf positionieren. Im nächsten Jahr dürfte es dann in den Trilog von EU-Kommission, Rat und Parlament gehen. Wir kämpfen für ein Verbot biometrischer Massenüberwachung im öffentlichen Raum, wie sie in China existiert.

DR. PATRICK BREYER

sitzt für die Piratenpartei im EU-Parlament. Der Jurist begann seine politische Laufbahn als Abgeordneter im Schleswig-Holsteinischen Landtag. Seit 2019 sitzt er in Straßburg. Breyer ist Mitglied im Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres und stellvertretendes Mitglied im Rechtsausschuss. Die Europäische Piratenpartei ist im EU-Parlament Mitglied der Fraktion Grüne/Europäische Freie Allianz. Außerdem engagiert Breyer sich gegen die Vorratsdatenspeicherung.

Das Interview führte

Christina Denz

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

SYNTHETISCHE DATEN UND DATENSCHUTZ – EINE MOMENTAUFNAHME

Omar Ali Fdal

Laut Schätzungen von Gartner werden synthetische Daten bis 2030 die Verwendung realer Daten in KI-Modellen vollständig ersetzen. Der rechtliche Rahmen für synthetische Daten ist dabei oft unklar. Daher ist es wichtig sich einen klaren Überblick über das Zusammenspiel von synthetischen Daten und Datenschutz zu verschaffen – damit sich Fortschritt und Gesetzgebung nicht in die Quere kommen und Innovationen gefördert werden.

Die Datenschutz-Grundverordnung (DSGVO) unterscheidet beim Schutz personenbezogener Daten zwischen Pseudonymisierung und Anonymisierung. Bei der gesetzlich vorgeschriebenen Pseudonymisierung muss der für die Datenverarbeitung Verantwortliche die Identität von den zu verarbeitenden Informationen trennen. Dazu werden die Informationen als Schutz vor einer erneuten Verknüpfung von der Identität getrennt und sicher aufbewahrt. So können beide Teile nicht wieder zusammengefügt werden, es sei denn, jemand ist dazu befugt. Die gesetzlich vorgeschriebene Pseudonymisierung ist ein Standard in der Datenschutz-Grundverordnung, der erfüllt werden muss, wenn Unternehmen personenbezogene Daten verarbeiten und in Einklang mit den Anforderungen der Datenschutz-Grundverordnung verwenden wollen. Die Verordnung enthält spezifische Anforderungen, wie dieser Zustand erreicht werden kann. Der Europäische Datenschutzausschuss und andere Gremien wie die ENISA haben ebenfalls Leitlinien zur Verfügung gestellt, wie der Standard der gesetzlichen Pseudonymisierung technologisch erfüllt werden kann.

Das Ziel der Anonymisierung von Daten besteht nicht nur darin persönliche Identifikatoren zu entfernen, sondern auch darin sicherzustellen, dass es unmöglich ist aus dem Rest der Daten zu bestimmen, wer eine Person ist. Zudem sollte dieser Prozess dauerhaft sein. In diesem Fall fallen wirklich anonymisierte Daten nicht in den Anwendungsbereich der Datenschutz-Grundverordnung.

Im Gegensatz zur gesetzlich vorgeschriebenen Pseudonymisierung wird in der wissenschaftlichen Gemeinschaft häufig darüber diskutiert, was eine wirkliche Anonymisierung von Daten ausmacht. Auch die Aufsichtsbehörden überarbeiten

häufig die Definitionen der Datenanonymisierung im Rahmen der gesetzlichen Bestimmungen. Diese Einordnung bleibt den Unternehmen selbst überlassen, und je nach Auslegung des Gesetzes können unterschiedliche Ergebnisse erzielt werden, die den Schutz der Privatsphäre nicht immer gewährleisten.

Die Privatsphäre ist ein Spektrum. Im Laufe der Jahre haben Experten eine Reihe von Methoden, Mechanismen und Instrumenten zum Schutz personenbezogener Daten entwickelt. Diese Techniken führen zu Daten mit unterschiedlichem Schutz der Privatsphäre und unterschiedlichem Risiko der Re-Identifizierung. Sie haben mit dem Inkrafttreten der Datenschutz-Grundverordnung an Popularität gewonnen.

Was sind synthetische Daten?

Synthetische Daten werden zunehmend verwendet, um die Anonymisierung der eigenen Datensätze zu erreichen. Synthetische Daten werden algorithmisch erzeugt, verhalten sich aber wie echte Daten. Generative Modelle lernen die statistische Verteilung in den Originaldaten und ziehen daraus künstliche Stichproben, um synthetische Daten zu erzeugen. Bei der Generierung synthetischer Daten wird die Beziehung zwischen den ursprünglichen und den synthetischen Datensätzen aufgehoben.

Synthetische Daten sind durch zwei Aspekte definiert. Erstens werden sie von Algorithmen künstlich erzeugt, d. h. sie haben keinen direkten Bezug zu realen Ereignissen oder Personen. Zum anderen stellen sie die Realität dar. Das ist wichtig, denn künstliche Daten, die nicht die Originaldaten widerspiegeln, sind für die Analyse nicht geeignet.

Datenschutz für synthetische Daten

Es wäre falsch anzunehmen, dass synthetische Daten von Risiken wie Re-Identifizierungsangriffen oder Datenschutzverletzungen ausgenommen sind. Die Deep-Learning-Modelle, die zur Erzeugung synthetischer Daten verwendet werden, können aufgrund ihrer großen Rechenkapazität komplexe Aufgaben lösen. Allerdings merken sie sich auch Merkmale in den Trainingsdaten. Letztlich können die gespeicherten Muster in den synthetischen Daten reproduziert werden, was zu Datenschutzverletzungen führen kann.

Allerdings ist auch hier zu beachten: Es gibt keine allgemeingültige rechtliche Definition dafür, was eine Re-Identifizierung technisch ausschließt. Einer Definition am nächsten kommt die Arbeit der WP29. Wenn Unternehmen die DSGVO-Definition von anonymisierten personenbezogenen Daten erfüllen wollen, empfiehlt die WP29 derzeit, synthetische Daten gegen die drei bekannten Angriffe auf die Privatsphäre zu testen, die eine Re-Identifizierung verhindern. Wenn die folgenden Fragen mit Nein beantwortet werden können, gelten die Daten als vollständig anonymisiert:

- Ist es möglich, eine Person durch Isolierung einzelner Datensätze zu identifizieren?
- Ist es möglich, mindestens zwei Datensätze, die sich auf dieselbe Person beziehen, innerhalb eines Datensatzes oder zwischen zwei getrennten Datensätzen zu verknüpfen?
- Ist es möglich, einzelne Attribute aus dem Datensatz abzuleiten?

Um die Sicherheit zu erhöhen, können den Synthesemechanismen zusätzliche Vertraulichkeitsschichten hinzugefügt werden, zum Beispiel Differential Privacy (DP). Modelle lernen die ursprüngliche Datenverteilung mit einem DP-Algorithmus, um synthetische Datensätze mit DP zu erzeugen.

Allerdings kann keine Technik einen perfekten Schutz der Privatsphäre garantieren, wenn die Daten anschließend verwendet werden sollen. Verordnungen wie die DSGVO verpflichten Unternehmen, die Restrisiken einer Re-Identifizierung zu bewerten – überlassen es ihnen aber auch, zu beurteilen, was das genau bedeutet. Datenschutz ist ein empirisches Feld; ohne Experten ist es schwierig, die Risiken zu berechnen. Doch die Erstellung einer Datenschutzbewertung ist zeitaufwändig. Je nach Komplexität des Anwendungsfalls kann es drei bis sechs Monate dauern den Datenschutz für synthetische Daten zu erforschen, zu entwickeln, zu testen und zu genehmigen.

Die Anbieter synthetischer Daten bieten häufig integrierte Datenschutzbewertungen an, um die Datenschutzbeauftragten bei der Beurteilung des Datenschutzes zu unterstützen. Statice beispielsweise hat zu diesem Zweck eine eigene Reihe empirischer Datenschutzbewertungen (anstatt System) entwickelt, den Statice Anonymeter, mit dem Datenschutzbeauftragte das Datenschutzrisiko synthetischer Daten auf der Grundlage der WP29-Empfehlungen messen können.

Worauf Datenschutzbeauftragte achten sollten

In den meisten Fällen benötigen Unternehmen mehr als eine Datenschutzmethode, um ihre Daten angemessen zu schützen. Je nach Anwendungsfall können sie mehrere Techniken kombinieren. Datenschutzbeauftragte müssen von Anfang an in das Datenprojekt einbezogen werden, um den Umfang des Anwendungsfalls, die Art der verwendeten Daten und die Art der gemeinsamen Nutzung zu verstehen.

Zunächst sollten die Datenschutzbeauftragten die wichtigsten Kennzahlen für die Bewertung des Schutzes synthetischer

Daten festlegen. Dazu sollten sie gemeinsam mit dem Entwicklungsteam alle relevanten Anwendungsfälle berücksichtigen, die sich in Zukunft ergeben könnten. Dazu können Pläne gehören das Projekt zu skalieren, Dritte einzubeziehen, internationale Datenübertragungen durchzuführen oder personenbezogene Daten im Datensatz zu speichern.

Synthetische Daten sind ein immer häufiger auftretendes Thema. Die Einführung steckt allerdings noch in den Kinderschuhen. Daher sollten Unternehmen, die sich für die Zusammenarbeit mit einem Anbieter synthetischer Daten entscheiden, Zeit in die Schulung ihrer eigenen Mitarbeiter:innen investieren und sicherstellen, dass sie die Technologie, ihre Grenzen und ihr wahres Potenzial verstehen.

In den ICO-Datenschutzempfehlungen heißt es, dass die Datenschutzbeauftragten eine Datenschutz-Folgenabschätzung durchführen sollten, um festzustellen, ob eine Datenschutzmethode angemessen ist. Die Bewertung sollte Folgendes berücksichtigen:

- Art, Umfang, Kontext und Zweck der Datenverarbeitung;
- Stand der Technik und die Kosten für die Umsetzung einer Datenschutzmethode;
- Risiken, die die Datenverarbeitung für die Rechte und Freiheiten des Einzelnen mit sich bringt.

Vorsicht ist besser als Nachsicht

Die Speicherung und (gemeinsame) Nutzung von Daten unter Wahrung der Privatsphäre ist eine Herausforderung. Unabhängig von der verwendeten Technologie ist es wichtig die Risiken zu verstehen. Es gibt immer Risiken für die Privatsphäre, die bei der Arbeit mit Daten berücksichtigt werden müssen.

Einige Techniken, wie z. B. die Verwendung von DV-Algorithmen, bieten einen stärkeren Schutz gegen eine erneute Identifizierung als herkömmliche Maskierungsmethoden. Sie sind daher eine hervorragende Möglichkeit den Datenschutz in die Datenverarbeitung zu integrieren. Darüber hinaus können Unternehmen mit den richtigen Tools auch Restrisiken abschätzen und die Datenschutzbestimmungen leichter einhalten.

Die Datenschutzgemeinschaft betrachtet synthetische Daten als ein weiteres gültiges Instrument im Bereich des Datenschutzes; ein Instrument, das bei richtiger Anwendung große Vorteile bieten kann.

ÜBER STATICE:

Statice entwickelt eine Datenschutztechnologie, mit der Unternehmen ihre datengetriebenen Innovationen beschleunigen und gleichzeitig die Privatsphäre von Einzelpersonen schützen können. Mithilfe von Anonymisierungssoftware können Unternehmen datenschutzkonforme synthetische Daten generieren, die für jede Form der Datenintegration, -verarbeitung und -verbreitung geeinet sind. Unternehmen aus der Finanz-, Versicherungs- und Gesundheitsbranche können so die Datenqualität steigern und dadurch ihre Wertschöpfungskette signifikant verbessern. Statice ermöglicht das Trainieren von Machine Learning Modellen, die Nutz7ung von Cloud-Infrastrukturen und das Teilen von Daten mit Partnern. Erfahren Sie mehr über Statice auf

▶ www.statice.ai

Über den Autor

Omar Ali Fdal
ist Chief Data Scientist & Head of Privacy Research bei Anonos und Mitbegründer von Statice.

Ende Oktober 2022 übernahm der US-amerikanische Datenschutz-Anbieter Anonos die Statice GmbH. Das gemeinsame Unternehmen bietet eine Plattform, die schnelle Dateneinblicke ermöglich und gleichzeitig den Schutz und die Nutzung von Daten verbessern will.

Statice

Anzeige

Jetzt 3 Monate ZD kostenlos testen.

ZD – Zeitschrift für Datenschutz

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

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

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 17,– jährlich.

beck-shop.de/go/ZD

Die große Zeitschrift zum Datenschutz

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

Geschaffen für die Unternehmenspraxis

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

Alles inklusive:

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

3 Hefte gratis

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

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 173613
facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht
C.H.BECK

NUTZER-, KONTEXT- UND SITUATIONS-ADÄQUATE VERARBEITUNG BY DESIGN

vor dem Hintergrund von Art. 25 DSGVO und der KI-Verordnung

Prof. Dr. Steffen Kroschwald

Digitalisierung, die den Alltag durchdringt, kann Menschen unabhängig von Alter, Wohnort, sozialer Herkunft und etwaiger Barrieren erreichbar machen, ein selbstbestimmtes Leben ermöglichen und ihnen Teilhabe verschaffen. Die digitale Dauerpräsenz birgt aber auch Risiken. Menschen können sich durch sie herausgefordert fühlen, Ängste und Unsicherheiten damit verbunden sein. Solche „Verletzlichkeiten" sind dabei häufig auch situations- und kontextabhängig. Schutz, Selbstbestimmung und Teilhabe für Menschen in verschiedenen „vulnerablen" Kontexten und Situationen können gestaltet werden. Etwa durch die „by Design"-Vorgaben des Datenschutz- und des zukünftigen KI-Rechts.

1. Digitale Gesellschaften, digitale Vulnerabilitäten?

Datenverarbeitung begleitet unseren Alltag nicht nur. Der Alltag selbst verschiebt sich, nicht zuletzt angetrieben durch die Corona-Pandemie und ihre Distanzzwänge, zunehmend ins Digitale. Eine solche „digitale Gesellschaft" bietet Vorteile aber auch neue Risiken. Und es verlagert sich Macht:[1] Die Verlagerung des Alltags in das Digitale erfordert enorme Datenmengen. Die digitalen Spuren, die wir hinterlassen, machen die digitale Gesellschaft auswertbar, verfolgbar und auch manipulierbar. Die Dauerpräsenz des Digitalen kann Menschen in unterschiedlichen demografischen und sozialen Kontexten, Lebensumständen und Situationen herausfordern, überfordern, Ängste und Unsicherheit schüren. In der digitalen Gesellschaft kann das Recht des Einzelnen, über die Verarbeitung seiner personenbezogenen Daten selbst zu bestimmen und gegen unbegrenzte Verarbeitung geschützt zu sein,[2] gar nicht unterschätzt werden.

Als soziale Wesen sind Menschen nicht nur autonom, sondern im selben Maße auch bedürftig und aufeinander angewiesen.[3] Neben die „klassische" Gewährleistung von Schutz und Selbstbestimmung gesellt sich damit ein Teilhabeinteresse und bestehen diesbezüglich Risiken: Wer an der digitalen Gesellschaft selbstbestimmt teilhaben will, muss Zugang zu ihr und ihren Gütern haben, benötigt z.B. einen Internetanschluss. Wer selbstbestimmt im Spiel gesellschaftlicher Interaktion „mitspielen" möchte, muss jederzeit wissen, was die Spielregeln sind, muss neue Begehrlichkeiten und Partikularinteressen erkennen und einordnen können sowie die Sprache der digitalen Gesellschaft verstehen. Wer Betroffenenrechte geltend machen möchte, muss zunächst einmal wissen, dass es sie gibt, seine Möglichkeiten diese geltend zu machen, und auch die Wege zu deren Durchsetzung kennen. Mit der digitalen Gesellschaft entstehen in Bezug auf Schutz, Selbstbestimmung und Teilhabe damit neue Verwundbarkeiten und Verletzlichkeiten: Digitale Vulnerabilitäten. Sie zeigen sich

[1] Roßnagel, MMR 2020, 222ff.

[2] BVerfGE 65,1, 43 (Volkszählung).

[3] So bereits Kamlah, Philosophische Anthropologie, Mannheim 1972, 95.

in der digitalen Gesellschaft in verschiedenen Dimensionen: Sowohl *individuell* als auch *strukturell* digital vulnerabel können Menschen in Lebens- und Wohnkontexten sein, wenn sie einerseits aufgrund ihrer persönlichen Wohnverhältnisse oder andererseits aufgrund ihres räumlichen Wohnorts erschwerten Zugang zum Internet haben. In manchen Lebenslagen situativ oder in bestimmten Kontexten vulnerabel können etwa ältere Menschen sein, die mit der Geschwindigkeit sich verändernder und neu entstehender Anforderungen des Digitalen überfordert werden. Oder Kinder, die wohl mit den Endgeräten und neuen Diensten aber nicht mit plötzlichen Bedrohungen digitaler Kommunikation umzugehen wissen. Auch digitalaffine Menschen können in der digitalen Gesellschaft gleichwohl situativ vulnerabel sein; wenn man sie z.B. in unerwarteten Situationen mit Informationen überlädt oder mit permanenten Entscheidungsanfragen zermürbt. Situative und kontextbezogene Vulnerabilität kann damit von gruppenbezogenen Verletzlichkeiten losgelöst sein.

2. Schutz, Selbstbestimmung und Teilhabe by Design?

Ebenso wie Vulnerabilität in der Gesellschaft, und damit auch in der digitalen Gesellschaft, vorangelegt ist, lassen sich darin auch Gestaltungs- und Widerstandskräfte, also Resilienzen zugunsten der Gewährleistungsziele, schaffen. Maßnahmen könnten bereits dort ansetzen, wo sich die digitale Gesellschaft aktuell noch entwickelt: Bei der Entstehung ihrer Technologie, aber auch ihrer grundlegenden technischen und gesellschaftlichen Infrastruktur, bei Grundentscheidungen in Bezug auf den Zugang zu ihren (Gemein-)Gütern sowie in Bezug auf ihre (Geschäfts-)Modelle und gesellschaftlich-demokratischen Prozesse. Schutz, Selbstbestimmung und Teilhabe in Bezug auf die vorangehend beschriebenen individuell, situativ und kontextbezogenen Vulnerabilitäten könnten insofern „by Design" hergestellt werden.[4] Derartige Regelungsansätze finden sich, neben vielen Weiteren, in Art. 25 DSGVO sowie in der aktuell im Entstehen befindlichen KI-Verordnung.[5]

2.1. ... nach Art. 25 DSGVO

Das Konzept „Datenschutz und Privatsphäre in das Design und den Betrieb, nicht nur von Technologie, sondern auch von Betriebssystemen, Arbeitsprozessen, Managementstrukturen, physischen Umgebungen und vernetzter Infrastruktur einzubauen", wurde so bereits in den 1990ern unter anderem von Ann Cavoukian unter dem Begriff „Privacy by Design" beschrieben.[6] Art. 25 DSGVO setzt hieran an, wenn technische und (!) organisatorische Maßnahmen sowohl zum Zeitpunkt der Festlegung der Mittel als auch zum Zeitpunkt der eigentlichen Verarbeitung gefordert werden. „By Design" richtet sich damit an Entscheider auf allen Ebenen eines Verantwortlichen,[7] die zur Ausgestaltung der Verarbeitung und der zugrundeliegenden (Geschäfts-)prozesse ansetzen.

Die zu treffenden Maßnahmen müssen nach Art. 25 Abs. 1 DSGVO geeignet sein die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. Geschützt werden sollen nach Art. 1 Abs. 2 DSGVO dabei Grundrechte und Grundfreiheiten. Neben dem Recht auf Schutz personenbezogener Daten i.S.d. Art. 8 GrCh sollen die in Art. 25 DSGVO angeordneten Maßnahmen auch dem Schutz weiterer Grundrechte,[8] etwa auf Bildung (Art. 14 GrCh), Nichtdiskriminierung (Art. 21 GrCh), sowie den Rechten von Kindern, älteren Menschen und Menschen mit Behinderung (Art. 24, 25 und 26 GrCh) dienen.

Verarbeitungsprozesse, die z.B. systematisch Menschen mit Behinderung ausschlössen, könnten mit der grundrechtlichen Gewährleistung ihrer Eigenständigkeit, ihrer sozialen und beruflichen Eingliederung und ihrer Teilnahme am Leben der Gemeinschaft kollidieren. Grundrechtspositiv sind demgegenüber Maßnahmen, die Menschen mit körperlich oder geistig bedingten Leseschwächen schützen, z.B. durch Verwendung von Datenschutzhinweisen in leichter Sprache. Maßnahmen für Systeme, die sich gezielt an ältere Menschen richten, könnten in datenschutzrechtlichen Entscheidungssituationen grundrechtsfördernd so umgesetzt werden, dass sie älteren Menschen für die betreffende Entscheidung genügend Zeit einräumen.

Zu treffen sind ferner geeignete Maßnahmen, die dafür ausgelegt sind Datenschutzgrundsätze der DSGVO wirksam umzusetzen und Anforderungen der Verordnung zu genügen. So verlangt Art. 12 Abs. 1 DSGVO Informationen und Mitteilungen in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache [...] insbesondere für Informationen, die sich speziell an Kinder richten".[9] Ähnliches gilt für das „Privacy by Design" von Einwilligungsprozessen nach Art. 7 Abs. 2 DSGVO. Eine Gestaltung, in der betroffenen Personen an den „Eingangstüren zur digitalen Gesellschaft", etwa bei der Registrierung zu Plattformen oder der Installation zentraler Endgeräte, kombinierte

[4] Vásquez/Kroschwald, MMR 2020, 219.

[5] COM (2021) 206.

[6] Cavoukian, Privacy by design, Identity in the Information Society 2010, 247ff.

[7] Vásquez, DuD 2022, S. 101.

[8] Lang, in: Taeger/Gabel, DSGVO BDSG TTDSG, 4. A. 2022, Art. 25 DSGVO Rn. 34.

[9] Roßnagel ZD 2020, 89f.

Datenschutzinformationen und Einwilligungen zugemutet werden, die sich auf alle Sachverhalte der Plattform und ihres Ökosystems beziehen, wären wohl kaum im Sinne des Art. 25 DSGVO.[10]

Entsprechend sind überdies Einwilligungen im Anwendungsbereich des TTDSG, insbesondere zu Cookies und Webanalyse- und Tracking-Tools, zu behandeln. Eindrücklich zeigt sich die Ausnutzung situativer Vulnerabilität etwa beim Einsatz von sogenannten „Dark Patterns" bei Cookie-Einwilligungen, die Menschen mit Informationen überladen, Aufmerksamkeit vom Datenschutz weglenken, u.a. durch „Nudging" steuern, an der Informationsgewinnung oder Entscheidung hindern sowie durch „Flatterhaftigkeit" oder das „Im Dunkeln Lassen" von Nutzern verunsichern.[11] Statt „Dark Patterns" wären zum Schutz vor Vulnerabilitäten helle „White Patterns" einzusetzen, die Menschen gerade situativ und kontextbezogen unterstützen rationale und transparenzbegründete Entscheidungen zu treffen. Oder aber, indem Prozesse an bestimmten Stellen gezielt verlangsamt, durch Voreinstellungen nach Art. 25 Abs. 2 DSGVO vor Folgen einer Überhastung geschützt oder informatorisch so reduziert werden, dass echte menschliche Entscheidungen möglich werden.

Zu Letzterem gehören auch die nach Art. 12 Nr. 7 DSGVO der Kommission per delegiertem Rechtsakt zur Bestimmung übertragenen Bildsymbole. Sie zielen nach Art. 12 Abs. 7 DSGVO gerade darauf ab „in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln". Entsprechend standardisiert und intuitiv erhöhen auch sie Schutz, Selbstbestimmung und Teilhabechancen.[12]

Schließlich kann auch die Umsetzung von Betroffenenrechten mehr oder weniger datenschutzfreundlich gestaltet sein. Nach Art. 12 Abs. 2 DSGVO muss der Verantwortliche der betroffenen Person die Ausübung ihrer Rechte „erleichtern". Hiermit wohl nicht vereinbar wäre eine Gestaltung, die Verbraucher von der Geltendmachung ihrer Betroffenenrechte abhält, etwa weil Prozesse Medienbrüche enthalten, abschreckend und komplex aufgemacht sind und Betroffene den hohen Aufwand oder gar scheinbare Nachteile scheuen.

Die erforderlichen Maßnahmen sind zuletzt nach Art. 25 Abs. 1 1. Hs. DSGVO im Einzelfall mit Blick auf individuelle aber auch situative Schutzbedarfe zu treffen (Abwägung). Bei Gesundheitstechnologien könnte so z.B. ein höherer technischer und organisatorische Aufwand für adäquate Aufklärung in Bezug auf ältere Menschen erforderlich sein. In der Folge könnten gerade in solchen Bereichen etwa persönliche Aufklärungsgespräche über die Datenverarbeitung statt bloßer Information an Schnittstellen von Endgeräten angezeigt sein.

2.2. … in der KI-Verordnung?

Seit 2021 liegt ein Vorschlag der EU-Kommission für eine Verordnung über Künstliche Intelligenz (KI-VO-E) vor. Ziel ist eine „sichere, vertrauenswürdige und ethisch vertretbare Künstlichen Intelligenz" (Ewg. 5). Auf den Begriff der „Verletzlichkeit" bezieht sich der Verordnungsentwurf dabei an mehreren Stellen ausdrücklich.[13]

Hauptadressat der Gestaltungsanforderungen ist regelmäßig ein Anbieter als Stelle, „die die Entwicklung und Herstellung eines solchen Systems in Auftrag gibt, um es unter eigenem Namen oder unter eigener Marke in Verkehr zu bringen". Der Anbieter ist nicht nur zur Einhaltung der Konformitätsanforderungen, sondern auch für das Qualitätsmanagement, die Konformitätsbewertung sowie weitere Maßnahmen verantwortlich (Art. 16ff. KI-VO-E), mit denen er technischen und organisatorischen Einfluss auf das System ausübt. Weitere Pflichten, etwa zur Überprüfung und Meldung, richten sich an weitere Stellen in der Lieferkette eines Produkts; z.B. an Bevollmächtigte, Einführer und Händler (Art. 25-27 KI-VO-E).

Durch Anlehnung an das europäische Produktkonformitäts- und -sicherheitsrecht wird die Einhaltung von „by Design-Pflichten" Stellen zugeordnet, die diese Verantwortlichkeit auch insbesondere technisch tragen und Einfluss auf die Gestaltung nehmen können. In dieser Hinsicht ist der KI-Verordnungsentwurf dem Ansatz des Art. 25 DSGVO, der sich nur an Verantwortliche richtet, überlegen.[14]

Art. 5 KI-VO-E bestimmt per se verbotene Praktiken „im Bereich der Künstlichen Intelligenz". KI-Systeme, die Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person einsetzen, etwa „Dark Patterns" oder Methoden des „Nudging", und die physische oder psychische Schäden zufügen können, sind ebenso verboten (Abs. 1 lit. a) wie die Ausnutzung von „Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen" oder die Verwendung von KI-Systemen durch Behörden oder in deren Auftrag zur „sozialen Bewertung".

Anforderungen des Verordnungsentwurfs richten sich maßgeblich an sog. Hochrisiko-KI-Systeme. Zu diesen gehören typische diskriminierungsgeneigte Bereiche, die „historische

[10] Roßnagel, MMR 2020, 227; strenger Kroschwald/Polenz, in: Brönneke/Föhlisch/Tonner, Das neue Schuldrecht, 2022, 185ff.,

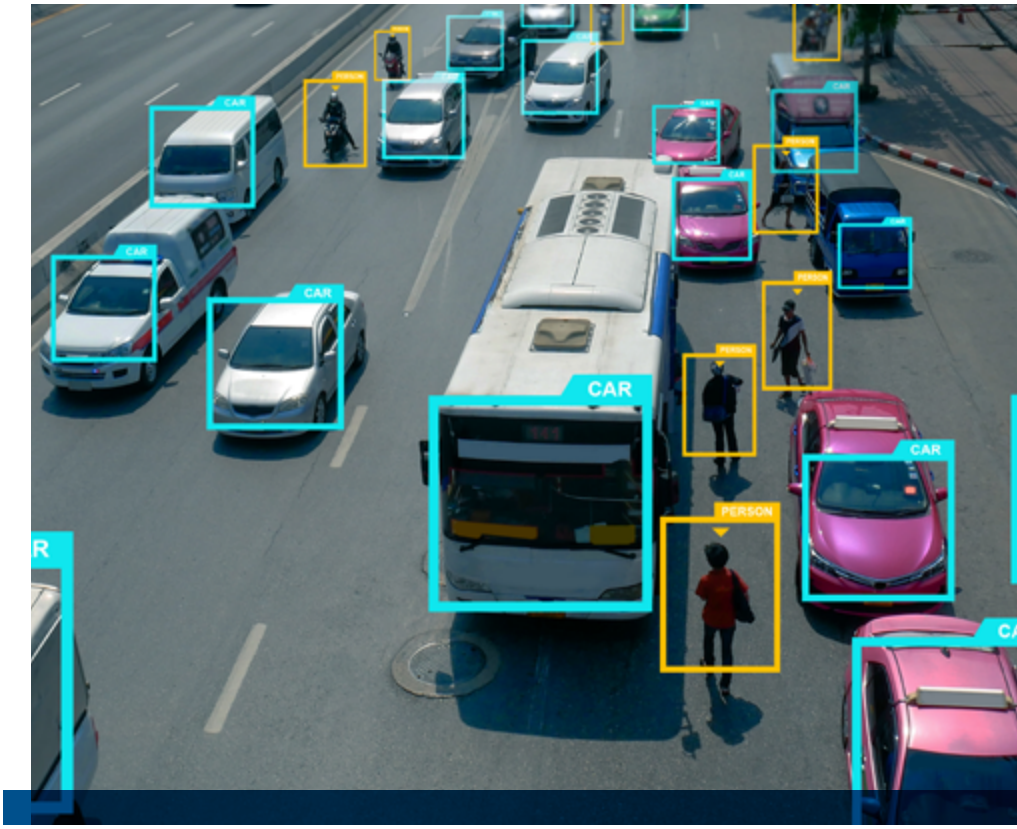
[11] Hierzu EDPB, Guidelines 3/2022.

[12] Vgl. Gutachten Datenethikkommission, 2019, 119.

[13] Geminn, ZD 2021, 354.

[14] Kroschwald, DUD 2022, 528.

Diskriminierungsmuster fortschreiben können“ (Ewg. 36), etwa den Zugang zu Bildung und die Bewertung von Schülern, den Zugang zu Beschäftigung, den Zugang zu und die Nutzung grundlegender privater und öffentlicher Dienste, die „die Abhängigkeit von Menschen in prekärer Lage ausnutzen können; etwa die Kreditwürdigkeitsprüfung oder die Sozialleistungskontrolle. Zu berücksichtigen sind dabei Schutzbedürftigkeiten „aufgrund eines Ungleichgewichts in Bezug auf Machtposition, Wissen oder wirtschaftliche oder soziale Umstände oder Alter“ (Art. 7 Abs. 2 lit. f KI-VO-E).



Besondere Bedeutung kommt im Zusammenhang mit KI dem Design einer vorgelagerten Trainings-, Test- und Validierungsphase zu. Da dadurch Verzerrungen (Biases) auftreten können, die unter anderem Diskriminierungsmuster replizieren, stellt Art. 10 KI-VO-E Anforderungen an die Daten- und Daten-Governance auf.[15] In ihr überschneiden sich im Falle personenbezogener Daten Anforderungen der KI-VO-E mit denen der DSGVO, insbesondere ihres Artikels 25.

Nach Art. 13 Abs. 1 KI-VO-E müssen Hochrisiko-KI-Systeme so konzipiert und entwickelt sein, dass ihr Betrieb hinreichend transparent ist. Nutzer, die mit KI-Systemen im Alltag interagieren, profitieren sodann von den Transparenzvorgaben unmittelbar. Etwa, dass Ergebnisse (und deren Genauigkeit, Art. 15 Abs. 2 KI-VO-E) für „die Nutzer“ interpretierbar und verwendbar sein müssen“ (Art. 13 Abs. 1 Satz 1 KI-VO-E). Dass nutzer- und situationsadäquate Information „auf eine geeignete Art und in angemessenem Maß“ (Abs. 1 Satz 2) präzise, vollständig, korrekt und eindeutig in einer für die Nutzer relevanten, barrierefrei zugänglichen (!) und verständlichen Form (Absatz 2) bereitgestellt werden muss. Und dass Nutzer einzelne Informationen (Art. 3 Abs. 3 KI-VO-E) zu Merkmalen des Systems, z.B. seiner Zweckbestimmung, erhalten sollen.

Unabhängig von der Einordnung als Hochrisiko-KI-System schreibt Art. 52 KI-VO-E Transparenzpflichten für bestimmte weitere KI-Systeme vor. So ist eine betroffene Person ggf. darüber zu informieren, dass sie es mit einem auf Interaktion ausgelegten KI-System zu tun hat, (Art. 52 Abs. 1 KI-VO-E), etwa beim Einsatz von Chatbots.[16] Ferner die Information, dass man als Person von Emotionserkennungssystemen betroffen ist (Abs. 2) oder Inhalte durch „Deepfakes“ als wahrhaftig erscheinen, obwohl sie durch entsprechende KI künstlich erzeugt wurden (Abs. 3).

Für den selbstbestimmten und teilhabeermöglichenden Umgang mit KI in digitalen Gesellschaften wird auch maßgeblich sein, dass an entscheidenden Stellen der Mensch in Prozesse integriert bleibt.[17] Bereits Art. 22 DSGVO zwingt den Menschen in den Entscheidungsprozess. Nach Art. 14 Abs. 1 KI-VO-E sind bei der Konzeption und Entwicklung von Hochrisiko-KI-Systemen „geeignete Werkzeuge einer Mensch-Maschine Schnittstelle“ zur Beaufsichtigung durch natürliche Personen zu gewährleisten. Diese gutgemeinte Aufsicht darf aber nicht in gefährlicher Überwachung münden. So etwa, wenn KI-Systeme, die in der Betreuung pflegebedürftiger Menschen in einer Weise beaufsichtigt werden müssen, dass die Aufsichtsperson permanent Einblick in die Privat- und Intimsphäre der zu betreuenden Person erhält.

[15] Hornung, DUD 2022, 561ff.

[16] Rostalski/Weiss, ZfDR 2021, 351.

[17] Kroschwald, DUD 2022, 527;

3. Liegt die Lösung im „Design“?

In Bezug auf Schutz, Selbstbestimmung und Teilhabe wirkt das Recht in zweifacher Richtung.[18] Zum einen, indem es Schutzzwecke vulnerabler Rechtssubjekte und damit auch die Vulnerabilität selbst mit definiert.[19] Zum anderen, indem es Maßnahmen zum Schutz und auch zur Herstellung von Resilienz und damit Selbstbestimmung und Teilhabe fordert oder fördert.

Schutzbedürftigkeit kann zunächst mit Elementen des Selbstschutzes begegnet werden – Sensibilisierung, Bildung und auch dem Kompetenzerwerb in Bezug auf die Digitalisierung. Ferner lassen sich eine Reihe von Transparenzanforderungen identifizieren, die auf adressaten- und situationsgerechte Gestaltung von Information in Produkten, Prozessen oder Systemen abzielen. Sowohl aus Art. 25 DSGVO als auch dem KI-Verordnungsentwurf lassen sich überdies neben Selbstbestimmungs- auch zahlreiche Teilhabegewährleistungen „by Design“ ableiten. Schließlich bedarf es auch der Rechtsdurchsetzung „by Design“ unter Berücksichtigung der Situation und des Adressatenkreises; etwa um zu verhindern, dass in Systemen angelegte Machtasymmetrien die Geltendmachung von Rechten erschweren.

Zu einem in der Regulierung angelegten Vorrang des Menschen („human centric design“) gehört schließlich auch der Auftrag Technologien selbstbestimmungs- und teilhabefördernd zu gestalten und zu entwickeln. Die im KI-Verordnungsentwurf z.B. angelegten „KI-Reallabore“ (Art. 53 KI-VO-E) oder andere „Regulative Sandbox-Enviroments“ könnten hierzu eine interessante Basis bieten.

Über den Autor

Prof. Dr. Steffen Kroschwald
ist Professor für europäisches und internationales Wirtschaftsecht an der Hochschule Pforzheim.
Er leitet das Zentrum Verbraucherforschung und nachhaltigen Konsum (vunk) der Hochschule Pforzheim und forscht zu Fragen der digitalen Selbstbestimmung und Teilhabe.

[18] Opolny ZRP 2022, 199

[19] Borowsky, in: Meyer/Hölscheidt, GrCh, 5. A. 2019, Titel 1, Vorb. Rn. 2.

Anzeige

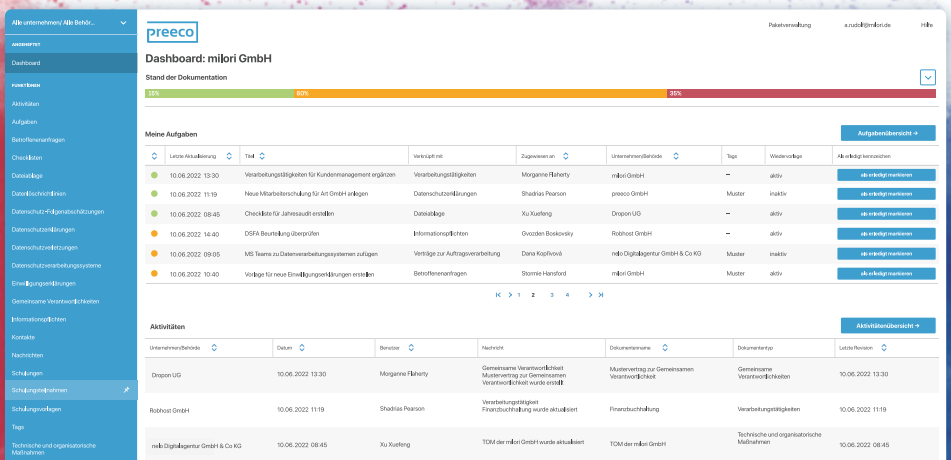
Kostenlos für BvD-Mitglieder: Zwei Stunden Premium Support

preeco

Software für besseren Datenschutz. Schafft Strukturen. Spart Zeit.

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

www.preeco.de/bvd



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

DAS RECHT AUF AUSKUNFT IN DER DATENSCHUTZ-GRUND-VERORDNUNG – ART. 15 DSGVO

Nicole Schmidt, LL.M., Elif Tüysüz

Die Datenschutzgrundverordnung regelt an verschiedenen Stellen die Rechte der betroffenen Personen. Betroffenenrechte werden definiert als Rechte, die der betroffenen Person Mit- und Einwirkungsmöglichkeiten auf ihre verarbeiteten personenbezogenen Daten gewährt. Auch pseudonyme Informationen werden als personenbezogene Daten eingestuft, da sie zwar nicht direkt, aber durch eine Transferleistung einer natürlichen Person zugeordnet werden können. Ausgenommen vom Anwendungsbereich der Datenschutzgrundverordnung sind anonyme Informationen, die keiner Person zugeordnet werden können.

Betroffenenrechte stehen der betroffenen Person zu. Darunter ist eine identifizierte oder identifizierbare natürliche Person zu verstehen (Art. 4 Nr.1 Hs.1 DSGVO).

Das **Recht auf Auskunft** nach Art. 15 DSGVO ist sicherlich das wichtigste Betroffenenrecht. Nach Erwägungsgrund 63 der DSGVO dient das Auskunftsrecht aus Art. 15 DSGVO der betroffenen Person dazu, sich der Verarbeitung seiner personenbezogenen Daten bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Die betroffene Person soll Umfang und Inhalt der gespeicherten Daten beurteilen können. Ferner dient die Auskunft dazu der betroffenen Person die Wahrnehmung der weiteren Rechte nach der Datenschutzgrundverordnung zu ermöglichen, vor allem das Recht auf Berichtigung nach Art. 16 DSGVO oder auf Löschung nach Art. 17 DSGVO.

Die betroffene Person hat nach Art. 15 DSGVO das Recht von dem Verantwortlichen eine Bestätigung darüber zu erhalten, ob sie betreffende personenbezogene Daten zum Zeitpunkt des Auskunftsverlangens überhaupt verarbeitet werden. Liegt ein Fall der Verarbeitung vor, so erstreckt sich das Recht auf zweiter Ebene darauf zu erfahren, welche sie betreffenden personenbezogenen Daten Gegenstand der Verarbeitung sind. Im Fall der Verarbeitung einer großen Menge von Informationen durch den Verantwortlichen sieht Erwägungsgrund 63 S.7 eine Präzisierungsmöglichkeit vor. Der Auskunftsanspruch ist nicht vererbbar (Die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW, 27. Tätigkeitsbericht 2022, S.101).

Form der Auskunft

Die **Erteilung** von Auskunft nach Art. 15 DSGVO kann auch per E-Mail erfolgen. Wegen Art. 12 Abs. 1 S. 2 DSGVO hat die Übermittlung der Information schriftlich oder in anderer Form, gegebenenfalls auch elektronisch, zu erfolgen. Eine Formbindung besteht gerade nicht. Im Fall der elektronischen Auskunftserteilung sind geeignete Schutzmaßnahmen zu treffen, so dass keine unbefugten Personen Kenntnis erlangen. Der Verantwortliche kann seine Auskunftspflicht auch elektronisch erfüllen, indem er der betroffenen Person einen Link zur Verfügung stellt, unter dem die Informationen

abgerufen werden können (vgl. LG München, Urteil vom 02.09.2021, Az.: 23 O 10931/20).

Der Verantwortliche kann sich zur Erfüllung seiner Verpflichtung auch Erfüllungsgehilfen bedienen. Wegen Art. 12 Abs. 1 DSGVO muss ein Verantwortlicher nur geeignete Maßnahmen treffen, damit die Mitteilungspflicht gemäß Art. 15 DSGVO erfüllt wird. Erteilt also eine Datenschutzbeauftragte Auskunft, so handelt es sich bei ihr um eine geeignete Erfüllungsgehilfin (vgl. LArbG Baden-Württemberg, Urteil vom 10.08.2022, Az.: 2 Sa 16/21).

Frist der Auskunftserteilung

Stellt der Betroffene einen zulässigen Antrag auf Auskunft nach Art. 15 DSGVO, so sollte der Verantwortliche dem Betroffenen wegen Art. 12 Abs. 3 DSGVO unverzüglich Auskunft erteilen, in jedem Fall aber **innerhalb eines Monats** nach Eingang des Antrags. Ist unter Berücksichtigung der Komplexität und der Anzahl von Anträgen eine Verlängerung der Frist erforderlich, so kann diese um zwei weitere Monate verlängert werden.

Inhalt der Auskunft

Die Auskunft muss die **Verarbeitungszwecke**, die **Empfänger von Daten** und die **geplante Dauer der Speicherung** enthalten. Unter den Auskunftsanspruch fallen Telefonnotizen, Aktenvermerke, Gesprächsprotokolle, E-Mails, Briefe sowie Kontobewegungen auf dem eigenen Bankkonto (vgl. OLG München, Urteil vom 04.10.2021, Az.: 3 U 2906/20; AG Bonn, 30.07.2020, Az.: 118 C 315/19). Der Bundesgerichtshof zählt auch eigene Korrespondenz der betroffenen Person und interne Vermerke zu „Daten", die in Kopie zu beauskunften sind (BGH, Urteil vom 15.06.2021, Az.: VI ZR 576/19). Nicht unter den Auskunfts- und Herausgabeanspruch aus Art. 15 DSGVO fallen dagegen Dokumente, die Vertragserklärungen enthalten (vgl. LG Berlin, Urteil vom 21.12.2021, Az.: 4 O 381/20).

Wurden keine personenbezogenen Daten der betroffenen Person beim Verantwortlichen verarbeitet, muss er eine **Negativauskunft** („es werden keine Daten verarbeitet") erteilen. Die Anfrage nicht zu beantworten ist unzulässig.

Der Verantwortliche stellt der betroffenen Person die verarbeiteten personenbezogenen Daten als **Kopie** zur Verfügung (Art. 15 Abs. 3 DSGVO). Der Herausgabeanspruch nach Art. 15 Abs. 3 DSGVO bezieht sich auf alle Daten, auf die das Auskunftsrecht nach Art. 15 Abs. 1 DSGVO gerichtet ist (vgl. LAG Niedersachsen, Urteil vom 22.10.2021, Az.: 16 Sa 761/20).

Erfüllung des Auskunftsanspruchs

Der Auskunftsanspruch wird dadurch erfüllt, dass der Auskunftspflichtige **seine Kenntnis** über die verarbeiteten personenbezogenen Daten **mitteilt**. Der Auskunftsanspruch ist auch dann erfüllt, wenn die Auskunft falsch ist, solange sie nicht von vornherein unglaubwürdig ist, so das LG Hagen mit Beschluss vom 31.08.2022. Das Gericht führt aus, dass der DSGVO-Anspruch auch dann erfüllt ist, wenn die erteilte Auskunft falsch oder unvollständig ist. Stellt die Auskunft im geschuldeten Gesamtumfang die Angaben nach dem erklärten Willen des Schuldners dar, so steht die etwaige inhaltliche Unrichtigkeit der Erfüllung nicht entgegen. Daher ist es für die Erfüllung des Auskunftsanspruchs wesentlich, ob der Erklärung des Verantwortlichen zu entnehmen ist, dass die Auskunft vollständig ist. Eine solche Erklärung ist dann anzunehmen, wenn die erteilte Auskunft erkennbar den Gegenstand des berechtigten Auskunftsbegehrens vollständig abdecken soll (vgl. LG Hagen, Beschluss vom 31.08.2022, Az.: 11 C 47/22). Auch nach der Auffassung des VG Bremen können unvollständige Auskünfte einen Auskunftsanspruch nach Art. 15 DSGVO erfüllen (VG Bremen 22.06.2022, Az.: 4 K 1/21).

Weiterhin führt das VG Bremen unter Verweis auf das Verwaltungsprozessrecht aus, dass sich der Kläger nicht auf eine fehlende Belehrung über die Betroffenenrechte in dem Auskunftsschreiben und damit auf mangelnde Kenntnis über die Betroffenenrechte berufen kann, wenn in dem Schriftsatz

zur Klageerhebung der Art. 15 Abs. 1 DSGVO vollumfänglich zitiert ist. Das Gericht vertritt hier die Auffassung, dass der Kläger auf diese Weise keine Verbesserung seiner Rechtsposition erreichen kann. Eine Klage, bei der nicht die Möglichkeit einer Verbesserung der eigenen Rechtsposition besteht, ist als rechtsmissbräuchlich zu bewerten und daher unzulässig.

Wann besteht kein Anspruch auf Auskunft nach Art. 15 DSGVO?

Der Auskunftsanspruch wird nicht dadurch ausgeschlossen, dass die gewünschten Auskünfte der betroffenen Person bereits bekannt sind (vgl. LG Bonn, Beschluss vom 24.05.2022, Az. 9 O 158/21). Ein Auskunftsanspruch aus Art. 15 DSGVO kann jedoch zurückgewiesen werden, wenn die Erfüllung dem Verantwortlichen **unzumutbar** ist. Liegt also ein grobes Missverhältnis zwischen Aufwand und Leistungsinteresse vor, so müsste dem Anspruch auf Auskunft nicht nachgekommen werden (vgl. AG Pankow, 28.03.2022, Az. 4 C 199/21).

Wird mit einem DSGVO-Auskunftsanspruch primär kein datenschutzrechtlicher, sondern ein anderweitiger Zweck verfolgt, ist das Begehren **rechtsmissbräuchlich**, wie das LG Kassel entschied (LG Kassel, Urteil vom 05.07.2022, Az.: 5 O1954/21). Der Antrag ist rechtsmissbräuchlich, wenn der Anspruch auf Auskunft dazu dient die Geltendmachung vermögensrechtlicher Ansprüche zu ermöglichen. Nach dem Erwägungsgrund 63 S. 1 DSGVO dient das Auskunftsrecht der betroffenen Person hinsichtlich der sie betreffenden personenbezogenen Daten dem Zweck sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können.

Ob der Auskunftsanspruch aus Art. 15 DSGVO nur für **datenschutzrechtliche Zwecke** besteht oder darüber hinaus auch anwendbar ist, konnte etwa das LG Erfurt (LG Erfurt, Hinweisbeschluss, 07.07.2022, Az. 8 O 1280/21) nicht beantworten und beabsichtigt daher den Rechtsstreit auszusetzen und eine Vorlage an den Gerichtshof der Europäischen Union vorzunehmen. Im Rahmen eines Vorabentscheidungsverfahren klärt der Europäische Gerichtshof unter anderem Auslegungsfragen, die von allgemeiner Bedeutung für die einheitliche Anwendung des EU-Rechts sind.

In einem gleichgelagerten Fall entschied jedoch das Oberlandesgericht Köln bereits, dass die Verfolgung verordnungsfremder Zwecke für sich nicht geeignet ist ein rechtsmissbräuchliches Vorgehen anzunehmen. Konkret wurde ein Kopieersuchen, mit dem sich die betroffene Person Informationen zur Vorbereitung eines Gerichtsverfahrens über datenschutzfremde Ansprüche gegen den Verantwortlichen beschaffen wollte, als unbedenklich und grundsätzlich zu erfüllen eingestuft (vgl. OLG Köln, 13.05.2022, Az.: 20 U 295/21).

Das Oberlandesgericht Nürnberg vertritt wiederum die Auffassung, dass Anträge auf Auskunft, die nicht der Überprüfung der Datenschutzkonformität, sondern anderen Zwecken dienen, rechtsmissbräuchlich sind und abgelehnt werden dürfen (OLG Nürnberg, 14.03.2022, Az. 8 U 2907/21). Rechtsmissbräuchlich ist die Geltendmachung eines Auskunftsanspruchs dann, wenn eine Einsichtnahme nicht der Prüfung von Art und Umfang der Verarbeitung personenbezogener Daten dient. Rechtsmissbräuchliche

Auskunftsgesuche sind nach Ansicht des OLG Nürnberg unter den Tatbestand der „exzessiven Anträge" nach Art. 12 Abs. 5 Satz 2 DSGVO zu subsumieren und rechtfertigen eine Weigerung Auskunft zu erteilen. Rechtmissbrauch wurde auch vielfach angenommen, wenn mit der Geltendmachung des Auskunftsanspruchs beispielsweise das Ziel verfolgt wird Informationen über Prämienanpassungen zu erhalten. Einem funktionswidrigen Auskunftsantrag, der der Vorbereitung eines Auskunftsbegehrens gegen den Verantwortlichen dient statt einer Verfolgung legitimer DSGVO-Ziele, muss nicht entsprochen werden (LAG Sachsen, Urteil vom 17.02.2021, Az.: 2 Sa 63/20).

Auch bei einer offensichtlichen Schikane des Verantwortlichen durch die betroffene Person in Form von sachfremden Drohungen, Verbalhornungen und Formalbeleidigungen ist von einem Rechtsmissbrauch auszugehen (AG Pforzheim, 05.08.2022, Az. 4 C 1845/21).

Einschränkungen des Auskunftsrechts können sich aus dem BDSG oder anderen deutschen Gesetzen ergeben. Möglich ist die Beschränkung des Auskunftsrechts auch durch die schutzwürdigen Interessen Dritter. Auch bei personenbezogenen Daten, die nur noch aufgrund von Aufbewahrungspflichten gespeichert werden (beispielsweise nach dem Steuer- oder Handelsrecht) oder die der Datenschutzkontrolle oder Datensicherung dienen, besteht auch dann kein Auskunftsanspruch, wenn die Erteilung der Auskunft einen unverhältnismäßigen Aufwand erfordert und die Zweckbindung durch geeignete technische und organisatorische Maßnahmen sichergestellt wird. Ob die Regelungen des § 34 BDSG, die das Auskunftsrecht einschränken, im Einklang mit der Datenschutzgrundverordnung stehen und angewendet werden können ist im Einzelfall zu prüfen.

Konsequenzen verspäteter oder unvollständiger Auskunft

Eine verspätete oder unvollständige Auskunft kann auch im Einzelfall ein Schadensersatz rechtfertigen. So hat sich das BAG in einer Entscheidung mit der Höhe eines Schadensersatzanspruchs nach Art. 82 Abs.1 DSGVO nach Geltendmachung eines Auskunftsbegehrens gemäß Art. 15 DSGOVO im Rahmen eines Arbeitsverhältnisses auseinandergesetzt. Hier haben die Richter geurteilt, dass die Schadensersatz-Höhe mit 1.000 Euro nicht zu beanstanden ist und somit nicht höher ausfallen muss (BAG, 05.05.2022, Az.: 2 AZR 363/21). Auch das OLG Brandenburg sah einen Streitwert von 1.000 Euro für einen Auskunftsanspruch, der dem Schutz immaterieller Grundrechtspositionen dient, als angemessen an (vgl. OLG Brandenburg, 01.08.2022, Az.: 12 W 23/22). Welcher Streitwert nun für die Geltendmachung anzusetzen ist, ist umstritten. Das Landgericht Bonn meint, dass der Anspruch auf Datenauskunft nicht verallgemeinerungsfähig mit einem pauschalen Streitwert bemessen werden kann. In aller Regel seien 500 Euro anzunehmen (vgl. LG Bonn, Urteil vom 01.07.2021, Az.: 15 O 335/20).

Das LG Köln argumentierte, dass nach Art. 82 Abs. 1 DSGVO jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadensersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter hat. Ist jedoch nicht ersichtlich, in welcher Weise der Betroffenen durch die Vorenthaltung einer Auskunft nach Art. 15 DSGVO einen immateriellen Schaden erlitt, so hat diese **keinen Anspruch** auf Schmerzensgeld (vgl. LG Köln, Urteil vom 22.06.2022, Az.: 25 O 9/22).

Gerichtlicher Rechtsbehelf gegen den Auskunftsverantwortlichen

Die betroffene Person kann gegen den Verstoß gegen das Auskunftsrecht gerichtlich im Wege einer Klage vorgehen. Die Klage ist hierbei bei dem Gericht des Mitgliedstaates einzulegen, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat oder in dem Staat, in dem die betroffene Person ihren Aufenthaltsort hat. In Deutschland sind für die Klagen gegen den Verantwortlichen die Zivilgerichte zuständig.

Über die Autorinnen

Nicole Schmidt, LL.M.
Rechtsanwältin, Geschäftsführerin SüdWest Datenschutz Rechtsanwaltsgesellschaft mbH

Elif Tüysüz
ist Studentin der Rechtswissenschaften an der Universität Mannheim mit dem Schwerpunkt Arbeitsrecht. Sie arbeitet als Werkstudentin bei der SüdWest Datenschutz Rechtsanwaltsgesellschaft mbH.

▶ https://www.suedwest-datenschutz.com

swds
DATENSCHUTZRECHT FÜR UNTERNEHMEN

Anzeige

PIA & ALFRIGHT

Die perfekte Kombi für alle Datenschutzbeauftragten

Hi, ich bin PIA.
Ihre digitale Datenschutzbeauftragte.

Mit mir erledigen Sie Ihre Aufträge als Datenschutzbeauftragter in 75% weniger Zeit und betreuen über 400 Kunden gleichzeitig!

- ✓ Intuitive Online Fragebögen für Datenschutzaudits
- ✓ Vollautomatisierte Erstellung der DSGVO Dokumentation inklusive Verzeichnis der Verarbeitungstätigkeiten und Dokumentation der technischen und organisatorischen Maßnahmen
- ✓ Zuordnung von praxisorientierten Handlungsempfehlungen
- ✓ Sensibilisierung der Mitarbeiter durch innovative E-Learning Kurse
- ✓ und vieles mehr

DSGVO APP

Hier erfahren Sie mehr über PIA: www.dsgvoapp.eu

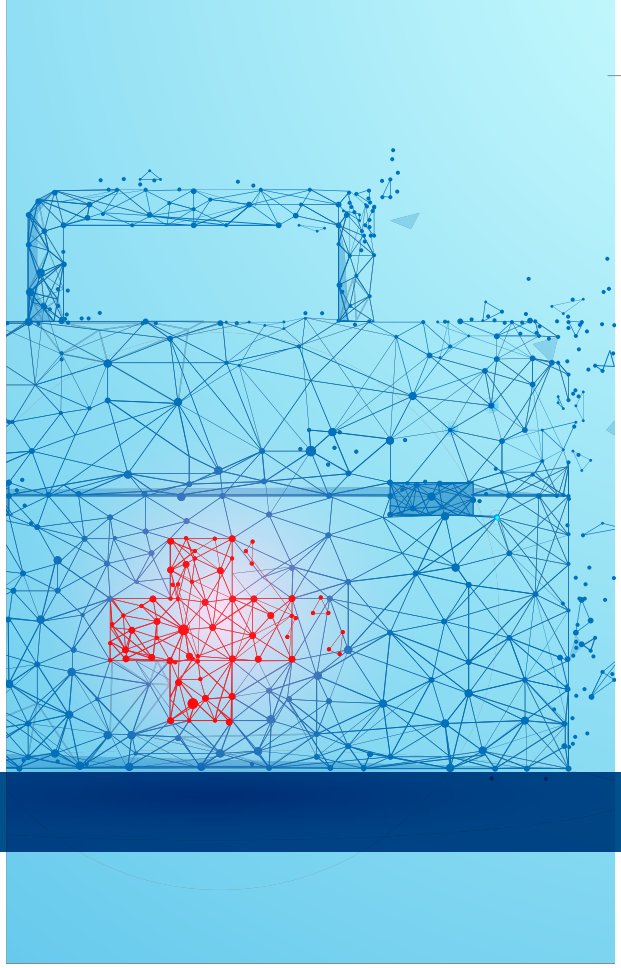
Hi, ich bin ALFRIGHT. Ihr DSGVO Website Butler.

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

- ✓ Vollautomatische Datenschutz-Analyse von Webseiten
- ✓ 100% Sicherheit hinsichtlich DSGVO, BDSG, EU-Cookie Richtlinie sowie TTDSG
- ✓ Erkennung von über 4.000 Cookies, externen Diensten und Consent Tools
- ✓ Automatisierte Erstellung und Aktualisierung der Datenschutzhinweise
- ✓ und vieles mehr

ALFRIGHT

Hier erfahren Sie mehr über ALFRIGHT: www.alfright.eu



CYBERSICHERHEIT IN DER „VUKA-WELT“

Ralf Rosanowski

Die Zahl der Cyberangriffe steigt seit Jahren. Die Angriffe richten sich gegen große Firmen genauso wie gegen kleine Familienunternehmen. Natürlich stehen aber auch Kommunen, Behörden und sogenannte KRITIS-Unternehmen im Fokus. Gleichzeitig leben wir alle in der „VUKA-Welt“, die es immer weniger erlaubt Schlüsse aus Entwicklungen in der Vergangenheit zu ziehen und langfristig strategisch zu planen. Wie gehen wir mit diesen Herausforderungen um? Wie kann man sich schützen? Wo findet man in Notfall Hilfe? Die Betrachtung von drei Thesen vermittelt Antworten auf diese Fragen.

These 1: Die rasche Wiederherstellung einer IT-Infrastruktur nach einem Ransomware-Angriff ist ein Mythos.

Nach einer Umfrage der Firma Sophos im Januar und Februar 2022 bei 5.600 IT-Profis in mittelgroßen Unternehmen in 31 Ländern wurden 66 Prozent der befragten Firmen 2021 Opfer eines Ransomware-Angriffs (+78 Prozent gegenüber 2020).[1]

Bei 65 Prozent aller Angriffe wurden Daten verschlüsselt. 46 Prozent der betroffenen Firmen haben daraufhin Lösegeld bezahlt. Durchschnittlich konnten daraufhin 61 Prozent der verschlüsselten Daten wiederhergestellt werden.

Letzteres hört sich zunächst viel an, heißt aber auch, dass 39 Prozent der Daten verloren sind! Zudem führt die ausschließliche Betrachtung der Datenmenge nicht zum Ziel. Wenn systemrelevante Daten wie das Active Directory zerstört sind, ist der Schaden immens.

Wo liegen nun die Probleme – und löst die Bezahlung von Lösegeld das entstandene IT-Problem nachhaltig?

Es mag für einen CEO vielleicht naheliegen Lösegeld zu bezahlen und zu hoffen, dass die Cyberversicherung die Lösegeldzahlung und den Betriebsausfall abdeckt, um möglichst rasch wieder in den Normalbetrieb der Firma zu kommen. Diese Überlegung greift jedoch viel zu kurz, weil sie – ungeachtet der Unsicherheit einer zeitnahen und vollständigen Wiederherstellung der verschlüsselten Daten – mit ganz erheblichen und überwiegend unkalkulierbaren IT-Sicherheitsrisiken einhergeht und schon aus diesem Grunde abzulehnen ist. Zudem: Gab es beispielsweise durch mangelhafte Dokumentation,

[1] Ransomware Hit 66% of Organizations Surveyed for Sophos' Annual "State of Ransomware 2022"

unklare Prozesse oder fehlende Notfallkonzepte Defizite in der bisherigen IT-Infrastruktur, so lassen sich diese gerade nicht durch die Bezahlung von Lösegeld kompensieren.

Bei einem kompromittierten System ist völlig unklar, ob noch unentdeckte Backdoors vorhanden sind, die es den Tätern erlauben sich erneut unerkannt im Firmennetz aufzuhalten und gegebenenfalls vertrauliche Daten auszuspähen. Letztendlich kann eine erneute Infizierung des Systems nach der Wiederinbetriebnahme selbstverständlich nicht ausgeschlossen werden. Zudem wird die Veröffentlichung von Daten im Darknet durch die Zahlung oftmals gar nicht verhindert.

Dessen ungeachtet wird mit einer Lösegeldzahlung die organisierte Kriminalität finanziert. Die dadurch – wie auch ein legaler Wirtschaftszweig – weiterwachsen kann und wird.

Im Grunde ist es nicht empfehlenswert ein nach Zahlung von Lösegeld entschlüsseltes System wieder in Betrieb zu nehmen – auch nicht nach mehreren Virenscans, die ohne Befund geblieben sind. Einem einmal kompromittierten System darf man nicht mehr vertrauen. So könnten unbemerkt Administrator-Accounts eingerichtet sein, die einen späteren Zugriff der Täter jederzeit möglich machen würden.

Ein Beispiel aus dem normalen Leben mag die Sachlage verdeutlichen: Wer einmal Opfer eines Wohnungseinbruchs geworden ist, wird zweifellos überlegen, wie das Wohnobjekt künftig besser geschützt werden kann und im Zweifel mehr Geld in bessere Sicherungstechnik investieren. Regelmäßig dürfte es daher nicht bei der bloßen Beseitigung offenkundiger Beschädigungen bleiben.

Für die IT gilt dasselbe. Es ist daher unvermeidbar das Gesamtsystem inklusive aller Client-Rechner neu aufzusetzen und dabei gleichzeitig die Sicherheitsstandards zu optimieren. All das kostet viel Zeit und Geld – zahlt sich aber auf längere Sicht in allen Fällen aus.

These 2: Es wird noch schlimmer, wenn wir nicht endlich konsequent handeln.

Nach einer Umfrage des Branchenverbands Bitkom bei Internetnutzern im Jahr 2021 wurden in den zurückliegenden zwölf Monaten acht von zehn Personen Opfer von Internetkriminalität.[2] Beim Angriffsziel deutsche Wirtschaft berechnete die Bitkom aktuell einen Gesamtschaden von 203 Milliarden Euro (gegenüber 223 Milliarden Euro im Jahr 2021) durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage.[3]

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) meldete in seinem Jahresbericht 2021 durchschnittlich rund 394.000 neue Schadprogrammvarianten – pro Tag!

Das Bundeskriminalamt meldete für das vergangene Jahr ein Plus von 12 Prozent bei den polizeilich registrierten Cyberstraftaten.[4]

Angesichts dieser alarmierenden Zahlen stellt sich die Frage nach einer Zukunftsprognose. Aus systemischen Gründen ist dies jedoch ausgesprochen schwierig. Auf die Hintergründe dazu werde ich in These 3 genauer eingehen. Es ist leider nicht so einfach möglich Entwicklungen aus der Vergangenheit in die Zukunft zu projizieren – selbst wenn es sich um scheinbar lineare historische Entwicklungen handelt. Ungeachtet der regelmäßig nicht erkenn- und nachprüfbaren Ursache-Wirkungsbeziehungen der publizierten Daten muss häufig auch die Validität der Daten kritisch hinterfragt werden. So stützen sich Veröffentlichungen vielfach auf Umfrageergebnisse. Selbst wenn diese Umfragen repräsentativ sind, so sind sie oftmals doch sehr subjektiv geprägt und entziehen sich daher regelmäßig einer Validierung. Die Daten der polizeilichen Kriminalstatistik sind in dieser Hinsicht zwar belastbarer – weil nicht von einer subjektiven Einschätzung geprägt, sie beschränken sich jedoch auf die polizeilich registrierte Kriminalität und lassen das Dunkelfeld (der nicht angezeigten Sachverhalte) unbeachtet.

Dennoch: Trotz aller Verzerrungsfaktoren ist über die letzten Jahre der ansteigende Trend unumstritten. Die ständig weiterwachsende Technologisierung durch verstärkte Homeoffice-Arbeitsplätze, die weitere Verbreitung des Internet der Dinge (Smart-Home-Lösungen), die zunehmende Automatisierung der Industrie (Industrie 4.0), das Anwachsen von E-Mobilität und autonomem Fahren und schließlich auch die Umsetzung des Onlinezugangsgesetzes dürfte mit Sicherheit weitere beziehungsweise größere Handlungsfelder für Cyberkriminelle eröffnen und als Verstärker wirken.

Auch wenn eine valide Prognose an dieser Stelle nicht leistbar ist, so sollte dennoch erkennbar sein, dass wir nicht umhinkommen künftig deutlich mehr Ressourcen als in der Vergangenheit in die Themen Cyber- und IT-Sicherheit zu investieren.

[2] Acht von zehn Personen werden Opfer von Internetkriminalität | Bitkom e.V.

[3] 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen | Bitkom e.V.

[4] BKA - Lageprodukte aus dem Bereich Cybercrime - Bundeslagebild Cybercrime 2021

These 3: Auch oder gerade in einer „VUKA-Welt" bedarf es eines strategischen Ansatzes der Leitungsebene.

Das Akronym VUKA (engl. VUCA) steht für die Begriffe

- Volatilität
- Unsicherheit
- Komplexität
- Ambiguität

Der ursprünglich aus dem militärischen Kontext stammende Begriff beschreibt heute unter anderem auch die schwierigen Rahmenbedingungen der Unternehmensführung.

Volatilität bezieht sich auf die zunehmende Häufigkeit, Geschwindigkeit und das Ausmaß von (meist unvorhersehbaren) Veränderungen (wie die Corona-Pandemie oder Lieferkettenunterbrechungen).

Unsicherheit steht für das generell abnehmende Maß an Vorhersagbarkeit von Ereignissen im privaten und beruflichen Leben (z. B. Wirtschaftswachstum, Inflation).

Komplexität bezieht sich auf die steigende Anzahl von unterschiedlichen Verknüpfungen und gegenseitigen Abhängigkeiten. Dadurch verlieren die Themen in unserem Leben ihre Berechenbarkeit und Planbarkeit. Häufig bestehen lediglich Korrelationen, aber keine Kausalitäten, die gewisse Rückschlüsse zulassen würden.

Ambiguität beschreibt die Mehrdeutigkeit der Faktenlage, die eine falsche Interpretation und entsprechende Entscheidungen wahrscheinlicher macht.

Wie soll man nun vorgehen in einer Welt, in der das Zurückliegende nicht direkt auf die Zukunft übertragbar ist und Strategien von heute eventuell schon morgen nicht mehr funktionieren können?

In unsicheren und komplexen Umfeldern bieten Leitbilder und Ziele Orientierung (VISION). Es ist Aufgabe der CEOs und Behördenleitungen, diese Vision mit Leben zu füllen. Ganz entscheidend wird es dabei darauf ankommen, die Frage „warum" es eine Firma oder Behörde gibt schlüssig und nachvollziehbar beantworten zu können.

Dabei gilt es Zusammenhänge selbst zu verstehen und verständlich zu machen (UNDERSTANDING). Es gilt den Kontext zu berücksichtigen und meta-strategisch zu denken und zu planen. Hierzu braucht es Zusammenarbeit, viele unterschiedliche Sichtweisen und gemeinsame Bilder.

Eine konkrete Sprache schafft Sicherheit und einen stabilen Rahmen (KLARHEIT). Was keinen Kontext hat, kann auch nicht klar sein. CEOs und Behördenleitungen müssen nötige Veränderungen oder die digitale Transformation ihres Unternehmens oder ihrer Behörde klar erläutern können.

In einer VUKA-Welt werden Planungshorizonte kürzer. Unternehmen und Behörden brauchen Konzepte, um sich schneller anzupassen oder auf neue Strategien auszurichten. AGILITÄT ist hierzu der Schlüssel. Agile Projekt- und Arbeitsmethoden erlauben die zeitnahe Anpassung des Vorgehens ohne das große Ziel aus den Augen zu verlieren.

Um auch in der Welt von morgen noch zweckmäßig agieren zu können, bedarf es resilienter Systeme und Organisationen. Um dies zu erreichen, müssen strategische Entscheidungen getroffen und umgesetzt werden. Die Pandemie und der russische Angriff auf die Ukraine mit ihren jeweiligen Auswirkungen (auch im Bereich der IT) haben einen Umdenkprozess angestoßen, dessen Ende noch nicht absehbar ist. Die bisherigen Denk- und Arbeitsmodelle einer globalisierten Welt mit einer Just-in-time-Produktion haben plötzlich nicht mehr wie gewohnt funktioniert. Dieser Umbruchprozess ist noch in vollem Gange.

Was ist nun zu tun?

An dieser Stelle gilt es je nach Reifegrad des Unternehmens oder der Behörde zu differenzieren zwischen Sofortmaßnahmen, die kurzfristig und ohne große finanzielle und administrative Aufwände realisierbar sind, aber nur beschränkte Wirkung entfalten und Maßnahmen, die nachhaltig und umfassend wirken, aber mit signifikantem personellen und finanziellen Einsatz verbunden sind.

Aus einer aktuellen Umfrage von Deutschland sicher im Netz e. V. (DsiN) zur IT-Sicherheit im Mittelstand[5] geht hervor, dass

- nur 49 Prozent der befragten Unternehmen ihre Systeme regelmäßig und so schnell wie möglich patchen oder updaten;
- nur 29 Prozent über ein Backup-Konzept verfügen und regelmäßig darauf zurückgreifen,
- 37 Prozent sogar ganz auf die Ermittlung von Risikofaktoren verzichten und
- 50 Prozent nicht einmal übertragene Dateien in Anhängen von E-Mails absichern.

Führt man sich vor Augen, dass in Baden-Württemberg 99 Prozent aller Unternehmen – das sind immerhin knapp 500.000 Firmen – der Kategorie kleine und mittlere Unternehmen (KMU) zuzuordnen sind, dann wirken diese Zahlen alarmierend.[6]

[5] DsiN-Praxisreport: 42 Prozent im Mittelstand melden IT-Angriffe | Deutschland sicher im Netz (sicher-im-netz.de)

[6] Mittelstandsbericht des Landes Baden-Württemberg 2021 (baden-wuerttemberg.de)

Bei einer solch dramatischen Ausgangslage sind in den betroffenen Firmen unverzüglich Notmaßnahmen zu treffen, um überhaupt einen gewissen Minimum-Standard an IT- und Cybersicherheit aufzubauen. Hierzu gehören:

- Zeitnahe Installation von Sicherheitspatches und Updates
- Nutzung starker Passwörter (am besten einen Passwortmanager verwenden)
- Konsequente Verwendung der Zwei-Faktor-Authentifizierung
- Nutzung einer aktuellen Virenschutzsoftware
- Einsatz einer Firewall
- Erstellung eines Backupkonzepts und Durchführung regelmäßiger Datensicherungen
- Sensibilisierung und Schulung von Mitarbeitenden (zum Beispiel zu Phishing und Social Engineering)

Die vorgenannten Maßnahmen stellen das absolute Minimum dessen dar, was – auch auf privaten Computern – unbedingt umgesetzt sein sollte. Unternehmen, bei denen die Existenz von einer funktionierenden IT-Infrastruktur abhängig ist, müssen natürlich über einen strukturierten Ansatz verfügen, der deutlich darüber hinaus geht.

Dringend zu empfehlen ist hierbei der Aufbau eines Information Security Management Systems (ISMS), das Regeln und Methoden definiert, um die Informationssicherheit in einem Unternehmen oder in einer Organisation zu gewährleisten (beispielsweise ISO 27000, VdS 1000, CISIS 12). CISIS 12 wurde speziell für den Einsatz in Kommunen und KMU entwickelt. Der IT-Planungsrat hat CISIS 12 offiziell für den Einsatz in der kommunalen Sicherheit empfohlen (aber ausdrücklich nicht für kritische Infrastrukturen!).

Ergänzend bedarf es der Anwendung und Umsetzung der Grundschutzkataloge des BSI und des Aufbaus und Betriebs eines leistungsfähigen Notfall- und Krisenmanagements, eines sogenannten Business Continuity Management (ISO 22301). Für Betreiber kritischer Infrastrukturen sind nach dem IT-Sicherheitsgesetz 2.0 ab dem 1. Mai 2023 unter anderem Detektionssysteme zur Angriffserkennung vorgeschrieben.

Die vorgenannten Maßnahmen erfordern regelmäßig den dauerhaften Einsatz finanzieller und personeller Ressourcen sowie oftmals die Beauftragung eines spezialisierten IT-Dienstleisters. Es ist nachvollziehbar, dass diese Dinge für kleine Familienunternehmen aber auch kleinere Kommunen sehr große Herausforderungen darstellen. Ohne entsprechende IT-Sicherheitsmaßnahmen wird es jedoch nicht möglich sein für die Herausforderungen der Zukunft gerüstet zu sein.

Welche Rolle hat die Cybersicherheitsagentur Baden-Württemberg?

Die Cybersicherheitsagentur Baden-Württemberg (CSBW) ist das Herzstück der neuen Cybersicherheitsarchitektur des Landes. Sie hilft Angriffe abzuwehren und den digitalen Raum für alle sicherer zu machen.

Mit dem Aufbau einer solch koordinierenden Stelle zur Vernetzung der bestehenden Cybersicherheitsstrukturen geht Baden-Württemberg als eines der ersten Bundesländer voran. Die Cybersicherheitsagentur ist zentrale Koordinierungs- und Meldestelle im Bereich Cybersicherheit in Baden-Württemberg. Sie sammelt ständig Daten zu Sicherheitslücken, Schadprogrammen und erfolgten oder versuchten Angriffen auf die Cybersicherheit. Hierfür nimmt sie auch direkt Meldungen von Betroffenen entgegen. Alles Relevante dokumentiert sie und wertet die Daten aus.

Für Behörden des Landes und an das Landesverwaltungsnetz angeschlossene Organisationen kann die CSBW auch Anordnungen treffen und Maßnahmen zu deren Schutz ergreifen.

CYBER-ERSTHILFE BW

Die Cyber-Ersthilfe der CSBW ist unter der Rufnummer 0711-137-99999 sieben Tage die Woche rund um die Uhr erreichbar.

Bei Cyberangriffen oder anderen Vorfällen kann die CSBW Landesbehörden, Städten und Gemeinden helfen – auch bei der Wiederherstellung der Systeme nach einem Angriff. In begründeten Einzelfällen können auch andere Organisationen mit wichtiger Bedeutung für das öffentliche Gemeinwesen Hilfe erhalten.

Im Herbst dieses Jahres startet die CSBW eine landesweite Sensibilisierungskampagne für Mitarbeitende der Landesverwaltung. Neben zahlreichen Informationsmaterialien kommt hierbei auch ein Computerspiel zum Einsatz, das die Mitarbeitenden auf spielerische Weise mit dem Thema IT- und Cybersicherheit vertraut macht (gamification Ansatz).

Über eine moderne Lernplattform werden künftig zudem zahlreiche Schulungsvideos und andere Lerninhalte für die Mitarbeitenden in der Verwaltung angeboten.

Für eine viel breitere Zielgruppe werden diese Angebote ergänzt durch Vorträge von Expertinnen und Experten aus der CSBW zu verschiedensten Themen im Bereich der Cybersicherheit und durch die Möglichkeit des Downloads von kostenlosem Informationsmaterial auf der Website:

▶ www.cybersicherheit-bw.de

Zum Jahresende 2022 wird die Website der CSBW in einem dann komplett neuen Design und mit vielen zusätzlichen Inhalten online gehen und das Präventionsangebot abrunden.

Gegenwärtig arbeiten wir mit Hochdruck daran ein Beratungs- und Unterstützungsangebot speziell zugeschnitten auf Kommunen zu erstellen und umzusetzen.

Im Koalitionsvertrag der Landesregierung wurde die Gefahr von Cyberattacken auf baden-württembergische Unternehmen mit Sorge gesehen. Um nun ergänzend zum vorgenannten Aufgabenportfolio auch Selbstständige und KMU besser bei der Cybersicherheit zu begleiten, bietet die CSBW künftig eine Erstberatung an. Ziel ist es, die Unternehmen in Baden-Württemberg zu sensibilisieren und Lösungswege für mehr Sicherheit in einer sich digitalisierenden Welt aufzuzeigen. Zur Umsetzung dieses Vorhabens laufen ebenfalls bereits erste Maßnahmen auch unter Konsultation der Industrie- und Handelskammern, der Handwerkskammern sowie von Verbänden und Institutionen. Aus wettbewerbsrechtlichen Gründen darf die CSBW bei der Erstberatung jedoch keine umfassende Risikoanalyse anbieten. Der Fokus liegt somit auf einer Erstbewertung des Unternehmens und dem Aufzeigen weiterer Handlungsschritte, die dann unter Beiziehung eines geeigneten IT-Dienstleisters erfolgen müssen.

Dessen ungeachtet versorgt die CSBW die Unternehmen in Baden-Württemberg bereits vorab mit anlassbezogenen technischen Handlungsempfehlungen und erstellt verschiedene Berichte.

Die Bedrohungslage ist – allen Verzerrungsfaktoren zum Trotz – relativ eindeutig und in der Fachwelt unumstritten. Woran es gegenwärtig noch mangelt ist die hinreichende Sensibilisierung von CEOs im Bereich der KMU und bei Leitungen von Behörden und Kommunen. Denn nur, wenn in den Leitungsbereichen ein ausreichendes Problembewusstsein für das Thema Cybersicherheit vorhanden ist, werden genügend Ressourcen bereitgestellt, um die offenkundigen Handlungsbedarfe anzugehen. Die CSBW hat daher in diesem Feld einen ihrer präventiven Aufgabenschwerpunkte.

Über den Autor

Ralf Rosanowski
ist seit September 2021 Präsident der damals neu gegründeten Cybersicherheitsagentur Baden-Württemberg. Zuvor war er Vizepräsident des Präsidiums Technik, Logistik, Service der Polizei Baden-Württemberg und Leiter der Abteilung 2, Informationstechnik.

▶ www.cybersicherheit-bw.de

LEO DESSANI, PROF. DR. RONALD PETRLIC

DANE ALS LÖSUNG FÜR SICHERE E-MAIL-ÜBERTRAGUNG

In der Anfangszeit der E-Mail-Kommunikation ging es primär um die Möglichkeit überhaupt elektronisch kommunizieren zu können. Das SMTP-Protokoll, nach dessen Vorgaben die E-Mail-Kommunikation abläuft, sah in der ursprünglichen Version keine verschlüsselte Übermittlung von E-Mails vor. Die Absicherung der Kommunikation war damals nicht so relevant wie heute. Mit der stetig zunehmenden Nutzung der E-Mail-Kommunikation in Wirtschaft und Wissenschaft, aber auch im Privaten, wurde der Sicherheit eine immer größere Bedeutung beigemessen. Seit einigen Jahren haben sich zahlreiche technische Standards zur Absicherung der E-Mail-Kommunikation durchgesetzt (1). Gleichzeitig haben immer mehr Mail-Server-Betreiber die verschlüsselte Übermittlung von E-Mails zwischen ihren Mail-Servern ermöglicht. Die Statistiken des Mail-Dienstes Gmail von Google bestätigen das: Zwischen Juli und Oktober 2022 wurden 87 Prozent aller ausgehenden und 91 Prozent aller eingehenden E-Mails transportverschlüsselt übertragen (2). Die Zahlen zeigen aber auch, dass längst nicht alle E-Mails verschlüsselt übermittelt werden. Das liegt daran, dass Mail-Server meist die sogenannte opportunistische Transportverschlüsselung unterstützen. Konkret bedeutet das, dass eine E-Mail nur dann transportverschlüsselt übermittelt wird, wenn beide Kommunikationspartner, also der sendende und der empfangende Mail-Server, TLS unterstützen. Wenn auf einem von beiden Mail-Servern kein TLS konfiguriert ist, wird die E-Mail unverschlüsselt übertragen. TLS ist das Verschlüsselungsprotokoll, das die Transportverschlüsselung ermöglicht.

Orientierungshilfe der Datenschutzaufsichtsbehörden

Mit der Intention, einheitliche Vorgaben in Bezug auf die E-Mail-Sicherheit zu machen, haben sich die Aufsichtsbehörden nach zähem Ringen (und gegen die Stimme Bayerns) im März 2020 auf eine Orientierungshilfe zur E-Mail-Sicherheit geeinigt;[1] sie wurde im März 2021 aktualisiert,[2] dabei wurden jedoch keine wesentlichen Änderungen vorgenommen. Die Orientierungshilfe ist nicht die erste Veröffentlichung staatlicher Stellen zur E-Mail-Sicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat bereits 2009 erste Empfehlungen zum "sicheren Betrieb von E-Mail-Servern" gegeben (3). Vor Kurzem hat das BSI das erste IT-Sicherheitskennzeichen an einen E-Mail-Provider auf Basis der Technische Richtlinie TR-03108-1[3] vergeben (4). Allerdings zeigt die Orientierungshilfe der DSK auf, welche konkreten Maßnahmen die Aufsichtsbehörden fordern. Diese Maßnahmen werden im Folgenden erläutert. Für Erklärungen zu den erwähnten Begriffen und Verfahren verweisen die Autoren auf ihre Website:

▶ https://mail-sicherheit.jetzt/blog/sicherheit-des-mail-oekosystems/

Zunächst unterscheidet die Orientierungshilfe zwischen dem Empfang und dem Versand von E-Mails. Im Detail unterscheidet sie weiter zwischen normalem und hohem

[1] vgl. https://mail-sicherheit.jetzt/wp-content/uploads/2021/07/orientierungshilfe_dks_email_2020.pdf, Letzter Zugriff: 03.10.2022.

[2] vgl. https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf, Letzter Zugriff: 03.10.2022.

[3] vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03108/TR03108-1.pdf?__blob=publicationFile, Letzter Zugriff: 07.10.2022.

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

LINKS UND LITERATUR ZUR SICHEREN E-MAIL

1. Chen/Paxson/Jiang (2020): Composition kills: A case study of email sender authentication. In: 29th USENIX Security Symposium (USENIX Security 20), S. 2183-2199.

2. Google-Transparenzbericht zur E-Mail-Verschlüsselung bei der Übertragung: https://transparencyreport.google.com/safer-email/overview.

3. Bundesamt für Sicherheit in der Informationstechnik: Sicherer Betrieb von E-Mail-Servern. BSI-Studie zur Internet-Sicherheit (2009): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_mail_server_studie_pdf.pdf?__blob=publicationFile&v=1,

4. IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/IT-Sicherheitskennzeichen/DE/2022/sik-01001_mail_de_freemail.html

5. Moriarty/Farrell (2021): RFC 8996, Deprecating TLS 1.0 and TLS 1.1. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/rfc8996/

6. Petrlic/Dessani (2021): E-Mail-Sicherheit auf dem Prüfstand: Forderungen der Aufsichtsbehörden vs. Absicherung in der Realität. In: Datenschutz und Datensicherheit, Ausgabe 8, S. 534-540.

7. Dessani/Petrlic (2021): Fehlender Vertrauensanker: Datenschutzprobleme bei Mailhosting-Anbietern. In: c't – magazin für computertechnik, Ausgabe 13, S. 132-137.

8. Google Workspace: Advancing email security for Gmail and beyond with BIMI. https://cloud.google.com/blog/products/identity-security/bringing-bimi-to-gmail-in-google-workspace, 2021.

Risiko. Der Risikobegriff wird in der Orientierungshilfe selbst nicht näher definiert, jedoch hat die Datenschutzkonferenz dazu bereits ein Kurzpapier[4] veröffentlicht.

Für den **Empfang von E-Mails mit normalem Risiko** müssen die Mail-Server laut der Orientierungshilfe mindestens eine opportunistische Verschlüsselung unterstützen; technisch wird das mit dem Verfahren START-TLS realisiert. Unverschlüsselte Verbindungsversuche können abgelehnt werden, eine Verpflichtung hierzu besteht aber nicht. Die verschlüsselten Verbindungen müssen mit sicheren Algorithmen nach dem Stand der Technik aufgebaut werden, die das BSI in der Technischen Richtlinie TR 02102-2[5] freigegeben hat. Konkret bedeutet das die Verwendung von TLS 1.2 und 1.3 mit sicheren Cipher Suites, nicht mehr aber TLS 1.0 und 1.1 (5). Zusätzlich muss für eingehende E-Mails – sofern vorhanden – die DKIM-Signatur überprüft werden, um sicherzustellen, dass die E-Mail von einem berechtigten Absender verschickt wurde.

Beim **Empfang von E-Mails mit hohem Risiko** fordert die Orientierungshilfe die Implementierung einer sogenannten "qualifizierten Transportverschlüsselung". Dabei müssen die eingesetzten TLS-Versionen – nach heutigem Stand – TLS 1.2 oder 1.3 sein und den Anforderungen der TR 02102-2 genügen sowie Perfect Forward Secrecy (PFS)[6] unterstützen. Außerdem müssen die Verantwortlichen die DNS-Einträge ihrer Domains mittels DNSSEC signieren und dafür sorgen, dass die Authentizität des Mail-Servers über einen zweiten Kanal überprüft werden kann. Was sich kompliziert anhört, ist im Endeffekt nichts anderes als die Konfiguration von DANE. Alternativ ist die Konfiguration von MTA-STS möglich, allerdings weist dieses Verfahren im Vergleich zu DANE einige Schwächen auf (6). Die Orientierungshilfe gibt zusätzlich vor, dass Verantwortliche den Empfang Ende-zu-Ende-verschlüsselter E-Mails ermöglichen müssen. Im besten Fall wird das durch Bereitstellen eines öffentlichen PGP- oder S/MIME-Schlüssels ermöglicht. Außerdem müssen Verantwortliche vorhandene PGP- oder S/MIME-Signaturen überprüfen.

Für den **Versand von E-Mails mit normalem Risiko** fordern die Aufsichtsbehörden in ihrer Orientierungshilfe zwingend eine verschlüsselte Übertragung der E-Mail ("obligatorische Transportverschlüsselung"). Demzufolge dürfen E-Mails nur dann versendet werden, wenn der Empfangsserver entsprechend der TR 02102-2 sichere TLS-Versionen unterstützt, also wieder TLS 1.2 oder 1.3 mit sicheren Cipher Suites.

Einen Schritt weiter gehen die Aufsichtsbehörden beim **Versand von E-Mails mit hohem Risiko**: Hier fordern sie "regelmäßig" eine qualifizierte Transportverschlüsselung. Eine E-Mail sollte also nur dann übertragen werden, wenn der empfangende Mail-Server TLS 1.2 oder 1.3 mit sicheren Cipher Suites, PFS und DANE bzw. MTA-STS unterstützt. Außerdem wird "regelmäßig" eine Ende-zu-Ende-Verschlüsselung gefordert. Wenn Verantwortliche also bei ausgehenden E-Mails sowohl eine qualifizierte Transportverschlüsselung als auch eine Ende-zu-Ende-Verschlüsselung einsetzen, sind sie auf der sicheren Seite.

[4] vgl. Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

[5] vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=4.

[6] Perfect Forward Secrecy (PFS) verhindert, dass eine aufgezeichnete verschlüsselte Kommunikation im Nachhinein entschlüsselt werden kann, und zwar auch dann, wenn der geheime Schlüssel ("Langzeitschlüssel") später versehentlich bekannt wird. Siehe auch: Claudia Eckert (2018): IT-Sicherheit. De Gruyter Oldenbourg, Berlin, 10. Auflage, S. 418.

Die von den Aufsichtsbehörden geforderten Maßnahmen sind zur besseren Übersicht in der folgenden Tabelle dargestellt:

	SMTP mit TLS (TLS 1.2 oder 1.3)	DKIM	Ende-zu-Ende-Verschlüsselung	Signaturprüfung	Obligatorische Transportverschlüsselung	Qualifizierte Transportverschlüsselung
Empfang, normales Risiko	ja, STARTTLS	Bei eingehenden Mails prüfen				
Empfang, hohes Risiko	ja		ja, im besten Fall öffentlichen Schlüssel bereitstellen	ja		ja
Versand, normales Risiko	ja				ja	
Versand, hohes Risiko	ja		ja			ja

Eine unmittelbare (rechtliche) Pflicht zur Umsetzung der geforderten Maßnahmen lässt sich aus der Orientierungshilfe nicht ableiten. Allerdings sind Verantwortliche u. a. nach Art. 32 DSGVO für die Sicherheit bei der Verarbeitung personenbezogener Daten nach dem „Stand der Technik" zuständig. Auch wenn die geforderten Maßnahmen in der Orientierungshilfe als Empfehlungen zu verstehen sind und es an mehreren Stellen Optimierungspotential gibt, stellen sie ein gutes Schutzniveau dar. Außerdem spiegeln sie die Sichtweise fast aller Aufsichtsbehörden wider und können insofern als guter Wegweiser verstanden werden.

Stand der Umsetzung der Orientierungshilfe

Nachdem bis Mitte 2021 keine Ergebnisse zum Stand der Umsetzung der Orientierungshilfe bekannt waren, entschieden sich die Autoren dieses Beitrags zu einer großflächigen Prüfung: Einerseits sollten namhafte Webhosting-Provider und große Anwaltskanzleien getestet werden, gleichzeitig sollte geprüft werden, ob die Aufsichtsbehörden ihre eigenen Vorgaben einhalten. Im Jahr 2022 untersuchte einer der Autoren dieses Beitrags, Prof. Dr. Ronald Petrlic, gemeinsam mit einer Studierendengruppe der TH Nürnberg zusätzlich die Umsetzung der Maßnahmen bei medizinischen Einrichtungen in Deutschland.[7]

Webhosting-Provider, die die Websites der Verantwortlichen in (eigenen) Rechenzentren bereitstellen, betreiben meist auch deren Mail-Dienst. Eine Untersuchung der Mail-Server namhafter Webhosting-Provider, die teilweise mehrere Millionen Domains hosten, lieferte daher einen guten Überblick über den Stand der E-Mail-Sicherheit bei Verantwortlichen (7).

Insgesamt testeten die Autoren 18 Webhosting-Provider. Alle Webhosting-Provider ermöglichten die opportunistische Transportverschlüsselung mittels STARTTLS und PFS. Bei allen Providern stand TLS 1.2 zur Verfügung, bei manchen sogar TLS 1.3. Leider unterstützten fast alle Provider auch die veralteten TLS-Versionen 1.0 und 1.1 oder gar den unsicheren TLS-Vorgänger SSL. DANE und eine obligatorische Transportverschlüsselung unterstützten nur jeweils zwei Provider. Somit setzte kaum ein Verantwortlicher, der einen (Auftragsver-

[7] Lange/Chang/Fiedler/Petrlic: An Email a Day Could Give Your Health Data Away. In: Data Privacy Management Workshop (DPM), 2022.

PRIVACYSOFT
Datenschutzmanagement as a Service

DATENSCHUTZ CAMPUS

ENTSCHEIDEND IST DAS WISSEN FÜR MORGEN.

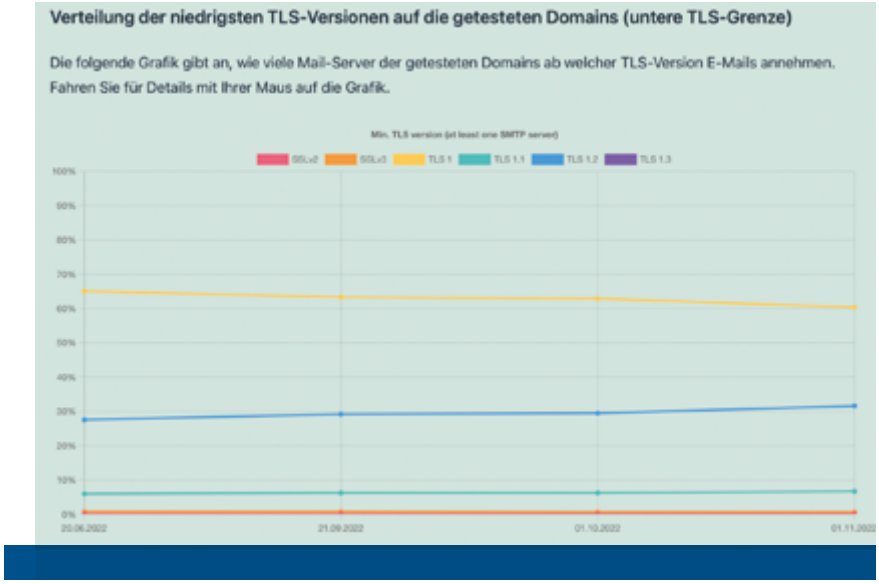
PRIVACYSOFT verfügt über eine integrierte eLearning Plattform über die wir Ihnen Web Based Trainings zur EU-Datenschutz-Grundverordnung anbieten.

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

arbeitungs-)Vertrag mit einem der getesteten Webhosting-Provider hatte, alle Forderungen der Orientierungshilfe um.

Auch Kanzleien waren Teil des Tests der Autoren (6). Insgesamt wurden sechs Kanzleien getestet. Deren Mail-Server unterstützten die opportunistische Transportverschlüsselung mittels STARTTLS und PFS sowie TLS 1.2, manche auch TLS 1.3. Leider konnten die Autoren bei den Mail-Servern einiger Kanzleien auch TLS 1.0 oder 1.1 oder gar SSL 3 feststellen. DANE wurde von keiner Kanzlei unterstützt, SPF von allen.



Aktuelle Testergebnisse stehen auf der Autoren-Website unter

▶ www.mail-sicherheit.jetzt/tests

zur Verfügung. Sie werden monatlich aktualisiert.

Vorschläge für die Praxis

Die in der Orientierungshilfe genannten Maßnahmen zur E-Mail-Sicherheit sind zum Teil praxisnah umsetzbar und dienen als guter Wegweiser. Allerdings vermissen die Autoren an einigen Stellen den Blick für die Praxis. Außerdem fehlen wichtige Verfahren zur Sicherung der E-Mail-Kommunikation oder werden nicht ausreichend beschrieben.

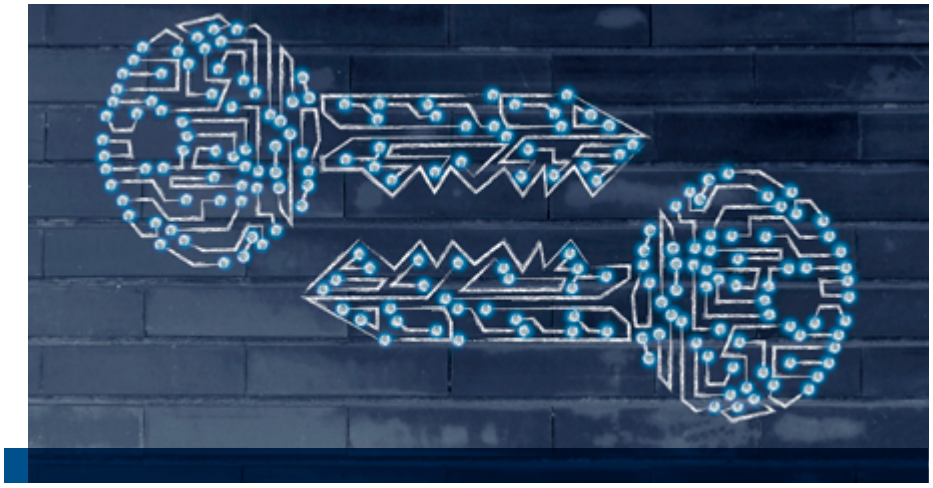
Auch bei den Aufsichtsbehörden des Bundes und der Länder waren die Ergebnisse durchwachsen (6): Alle unterstützten opportunistische Transportverschlüsselung mittels STARTTLS und PFS. Bei allen Behörden war mindestens TLS 1.2 konfiguriert, teilweise auch 1.3. DANE unterstützten allerdings nur wenige. SPF war nicht bei allen Behörden konfiguriert, obwohl das seit Langem zum Stand der Technik gehört (1). Zwar existieren bei den Behörden teilweise Abhängigkeiten von der IT-Infrastruktur der Länder, dennoch zeigte sich in den Tests der Autoren, dass die Aufsichtsbehörden ihre eigenen Forderungen an die E-Mail-Sicherheit nicht vollständig umsetzen.

Der Stand der E-Mail-Sicherheit bei medizinischen Einrichtungen in Deutschland war wie folgt: Die Unterstützung von STARTTLS war mit 99,5 Prozent aller getesteten Mail-Server erwartungsgemäß hoch. Des Weiteren unterstützten 99,5 Prozent die aktuellen TLS-Versionen 1.2 und 1.3. Die Verfügbarkeit von DANE war mit ~0,9 Prozent aller getesteten Mail-Server allerdings sehr gering. Nur 25 von 2836 analysierten Mail-Servern – die von 81 verschiedenen medizinischen Einrichtungen genutzt werden – waren vollständig mit DANE geschützt und erfüllten damit die Anforderungen der Aufsichtsbehörden für E-Mail-Kommunikation mit hohem Risiko. Alle anderen medizinischen Einrichtungen dürften entsprechend den Vorgaben der Aufsichtsbehörden beispielsweise keine Gesundheitsdaten nach Art. 9 Abs. 1 DSGVO per E-Mail übermitteln, es sei denn, sie setzen weitere technische Schutzmaßnahmen ein wie eine Ende-zu-Ende-Verschlüsselung mittels PGP oder S/MIME ein. In der Praxis dürfte das unter anderem aufgrund der schlechten Benutzerfreundlichkeit und der hohen Komplexität nicht realistisch umsetzbar sein.

Die Forderung nach Ende-zu-Ende-Verschlüsselung ist nicht wirklichkeitsnah. Zwar wäre der großflächige Einsatz von Ende-zu-Ende-Verschlüsselung wünschenswert – in der Praxis nutzt aber kaum eine Privatperson Verfahren wie PGP oder S/MIME[8], sodass allein schon der Bezug des öffentlichen Schlüssels vom Kommunikationspartner scheitern dürfte. Anstelle der Ende-zu-Ende-Verschlüsselung sprechen sich die Autoren für den großflächigen Einsatz von DANE aus: Damit kommt man einer obligatorischen Transportverschlüsselung sehr nahe und kann gleichzeitig sicherstellen, dass eine E-Mail tatsächlich an den richtigen Mail-Server übermittelt wird. DANE ist ein Verfahren, das vom Administrator des Mail-Servers aktiviert und konfiguriert werden muss, also meist vom Webhosting- oder Mail-Provider. Der Endnutzer hat keine Möglichkeit das Verfahren selbst zu aktivieren – was den Vorteil hat, dass er sich nicht in die Details der Konfiguration einarbeiten muss.

Darüber hinaus gehören zu einem Mail-Setup, das dem Stand der Technik entspricht, mindestens das Signieren von ausgehenden E-Mails mit DKIM und das Einrichten von SPF so-

[8] Christian Stransky, Oliver Wiese, Volker Roth, Yasemin Acar und Sascha Fahl (2022): 27 Years and 81 Million Opportunities Later: Investigating the Use of Email Encryption for an Entire University. In 43rd IEEE Symposium on Security & Privacy. IEEE Computer Society.



wie DMARC, um Spam-Mails mit einem Absender der eigenen Domain erkennen zu können. Diese Maßnahmen werden in der Orientierungshilfe leider nicht beschrieben; sie sind aber für eine zeitgemäße Absenderauthentifizierung relevant.

Für noch mehr Sicherheit lohnt sich ein Blick auf ein vielversprechendes, aktuell aber noch junges Verfahren: BIMI ermöglicht es, eine Bildmarke – beispielsweise das Logo eines Unternehmens – als Icon beim Empfang von E-Mails anzuzeigen und wird unter anderem bereits von Gmail unterstützt (8). Dabei wird gewährleistet, dass nur der Markeninhaber ein gültiges Icon anzeigen kann. Wird also eine Spam-Mail von einer gefälschten Adresse versendet, ist für den Empfänger unmittelbar erkennbar, dass die E-Mail nicht authentisch ist. BIMI setzt SPF, DKIM, DMARC und die Eintragung einer Bildmarke in einem Markenregister voraus, weswegen die Implementierungskosten aktuell nicht gering sind.

Über die Autoren

Leo Dessani
ist Mitarbeiter am Lehrstuhl für Rechtsinformatik der Universität des Saarlandes. Er war im Sommersemester 2022 Lehrbeauftragter für IT-Sicherheit an der Hochschule Reutlingen und ist seit dem Wintersemester 2022/2023 Lehrbeauftragter für IT-Sicherheit und Datenschutz an der Deutschen Universität für Verwaltungswissenschaften Speyer. Sein Forschungsinteresse liegt in den Bereichen technischer Datenschutz, Privacy-Preserving Machine Learning und Sicherheit von Rechnernetzen.

Prof. Dr. Ronald Petrlic
ist seit 2020 Professor für Informationssicherheit an der TH Nürnberg. Davor war er Leiter des Technik-Referats beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg. Er ist Autor zahlreicher wissenschaftlicher Artikel, Gesetzes-Kommentare und des ersten Lehrbuchs zu „Privacy by Design".

Um die E-Mail-Kommunikation sicher zu machen ist eine regelmäßige Überprüfung der eingesetzten Techniken nötig. Die Autoren betreiben unter ▶ www.mail-sicherheit.jetzt ein Portal für das Voranbringen der E-Mail-Sicherheit in der Praxis, auf dem sich Tipps dazu finden.

PRIVACYSOFT
Datenschutzmanagement as a Service

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

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

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

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

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

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

DATENHANDEL IM SPANNUNGSFELD VON DSGVO, DGA UND DA

Dr. Kristina Schreiber

Wie können Unternehmen Daten rechtskonform und kommerziell erfolgreich nutzen, handeln und monetarisieren?

Die Bedeutung der Datenwirtschaft nimmt fortlaufend zu. Schon heute nutzen unzählige Unternehmen Daten für die Optimierung ihrer Geschäftsmodelle, für die Entwicklung neuer Geschäftsmodelle und etwa auch zur direkten Monetarisierung im Datenhandel. Ausgeschöpft haben bisher indes nur wenige Unternehmen den kommerziellen Wert von Daten. Ein Hindernis liegt in unklaren rechtlichen Vorgaben, die Regulierung dieser Datennutzung ist undurchsichtig: Zum einen fehlt es nach wie vor an klaren gesetzlichen Kriterien der Verfügungsmacht über Daten. Zum anderen nehmen die regulatorischen Vorgaben zu, beginnend mit der EU-Datenschutzgrundverordnung (DSGVO) hin zu den diversen neuen EU-Digitalrechtsakten, insbesondere der Datenstrategie (Data Governance Act und Data Act). Die Durchsicht durch diese Regulatorik ist eine Herausforderung, bietet aber zugleich enorme Chancen für Unternehmen durch eine proaktive Gestaltung eine kommerziell optimierte und rechtskonforme Datennutzung nach ihren Vorstellungen zu realisieren.

Daten sind aus diversen Geschäftsmodellen nicht mehr wegzudenken. Laufend entstehen neue Optionen einer Datenmonetarisierung, auch vormals rein analog tätige Unternehmen ergänzen ihre Produkte um digitale Elemente und benötigen hierfür Daten. Bei einem so verstandenen Datenhandel geht es um deutlich mehr als einen Adresshandel oder Handel mit Kundendaten. Ausgetauscht und genutzt werden hier Datensätze für Analysen oder die Anreicherung von Produkten, die so die gewünschten Leistungen erbringen können: Algorithmen für intelligente Anwendungen wollen trainiert werden, Apps benötigen Daten zur Wetterprognose oder die Stauumfahrung, Gesundheitsdaten werden für die Versorgungsforschung benötigt, eine Betrugsprävention kann mit Hinweisen auf Betrugsfälle optimiert werden und Informationen über die Produktverwendung ermöglicht eine Verbesserung der nächsten Produktgeneration. Ein so verstandener Datenhandel, wie er in der Praxis aktuell zunehmend auftritt, ist mithin deutlich mehr als der im Datenschutzrecht traditionell diskutierte Adresshandel. Oftmals ist ein solcher Datenhandel auch nicht auf personenbezogene Daten angewiesen, sondern operiert mit aggregierten und anonymisierten Datensätzen, Testfällen oder jedenfalls pseudonymisierten Daten.

Unklare rechtliche Vorgaben

Die Regulierung dieser Datennutzung nimmt dabei stetig zu: Im Rahmen der EU-Digitalstrategie verkündet Brüssel in einem zunehmenden Tempo neue Rechtsakte, zumeist unmittelbar geltende EU-Verordnungen. Diese müssen, anders als EU-Richtlinien, nicht zunächst in nationales Recht umgesetzt werden. Ab ihrem Geltungsbeginn müssen sich Unternehmen, Behörden und natürliche Personen in der EU an sie halten.

Bereits seit Mai 2018 ist insofern die DSGVO anwendbar, die für personenbezogene Daten den Maßstab für jegliche Verarbeitung setzt. Für nicht-personenbezogene Daten ist die (in der Praxis nur bedingt relevante) Free Flow of Data-Verordnung (EU) 2018/1807 zu beachten. Eine möglichst zugängliche Verarbeitung von Informationen des öffentlichen Sektors, dem Konzept des „Open Data" folgend, regelt die sog. Open Data-Richtlinie (EU) 2019/1024, die bis Sommer 2021 in nationales Recht umzusetzen war. Im Sommer 2022 ist als Teil der EU-Datenstrategie, einer Säule der Digitalstrategie, der Data Governance Act (DGA) veröffentlicht worden, an den sich Unternehmen und Behörden ab September 2023 halten müssen. Auch dieser „Act" ist eine unmittelbar in allen Mitgliedstaaten der EU geltende Verordnung (EU) 2022/868. Im Entwurf diskutiert wird aktuell der Data Act (DA), ebenfalls Teil der EU-Datenstrategie. Während sich der DGA vor allem mit der Weiterverwendung von Daten der öffentlichen Hand und nicht-kommerziellen Verarbeitungsformen (Datenmittler, altruistische Datenorganisationen) beschäftigt, wird der DA in fast alle Bereiche der Datennutzung hineinwirken mit Regelungen u.a. zur Missbrauchskontrolle von Verträgen über die Datennutzung, Datenübermittlungen in Drittstaaten, Interoperabilitätsvorgaben, Pflichten zur Datenportabilität, Datenbereitstellung und Zugangsgewährung sowie einer Pflicht Daten öffentlichen Stellen z.B. in Notfallsituationen bereit zu stellen. Kurzum: Kommt der DA, wie von der Kommission vorgeschlagen, so werden Anbieter von digitalen Produkten Nutzern automatisierten Zugang zu Metadaten gewähren müssen, die Migration zu anderen Diensten zu erleichtern haben und Verträge über die Datennutzung bei Beteiligung von kleinen und mittleren Unternehmen auf einen fairen Ausgleich hin zu überprüfen haben.

Die Regulierungsvorgaben sind insofern mannigfaltig und kaum noch zu durchblicken. Der Kern aber für eine zivilrechtliche Ausgestaltung der Datennutzung, die Frage der Verfügungsgewalt über Daten, ist nach wie vor ungeregelt und in der Diskussion. Der zivilrechtliche Eigentumsbegriff ist nach vorherrschender Ansicht auf körperliche Sachen beschränkt. Ein „Dateneigentum" im Sinne eines Ausschließlichkeitsrechts an den betreffenden Daten existiert jedenfalls noch nicht und wird auch absehbar nicht kommen. Für den Handel mit Daten kommt es daher in erster Linie auf den faktischen Zugriff an, Begrenzungen erfordern eine klare und durchsetzbare vertragliche Regelung – klare gesetzliche Vorgaben gibt es insofern nämlich nicht.

Dass weder der deutsche noch der EU-Gesetzgeber eine klare Zuordnung von Daten durch ein originäres Schutzrecht vorgenommen haben, führt dazu, dass für den Zugriff und die Verwertung von Daten auf tradierte Rechtsbereiche zurückzugreifen ist: Die Grenzen des rechtlichen Gestaltungsspielraums werden durch das Datenschutz- und Urheberrecht, den Schutz von Geschäftsgeheimnissen sowie das Straf- und Zivilrecht abgesteckt. Auch das neue digitale Regulierungsrecht, das „Datenrecht" der EU, ist künftig zu berücksichtigen. Innerhalb dieser Eckpfeiler verbleibt den Vertragsparteien ein erheblicher Gestaltungsspielraum, der mangels klarer gesetzlicher Regelungen auch genutzt werden sollte, um rechtssichere Lösungen zu finden.

Bestimmung der Datenart, Datenquelle und der Ziele

Ausgangspunkt jeder rechtlichen Überlegung, die maßgebliche Weichenstellung, ist dabei die Bestimmung der Datenarten, mit denen gehandelt werden soll, und die Herkunft dieser Daten. Nur bei personenbezogenen Daten ist das Datenschutzrecht anwendbar; die Herkunft der Daten ist entscheidend für etwaige Nutzungsbeschränkungen aus urheberrechtlicher Sicht und – bei personenbezogenen Daten – angesichts der datenschutzrechtlichen Zweckbindung für die zulässige Weiterverarbeitung.

Personenbezogene und nicht-personenbezogene Daten

Ein Datenhandel kann sich auf personenbezogene oder auch nicht-personenbezogene Daten beziehen. Wann immer möglich sollte dabei auf den Handel mit personenbezogenen Daten verzichtet werden: Diese sind durch das Datenschutzrecht in besonderem Maße geschützt, bei Verstößen gegen das Datenschutzrecht drohen Bußgelder und Schadensersatzforderungen. Insbesondere aber ist eine Verarbeitung datenschutzrechtlich ohnehin allenfalls dann erlaubt, wenn die Verarbeitung erforderlich und notwendig für die Zweckerreichung ist – in vielen Fällen aber lassen sich Analysen und weitere Ziele der Datennutzung auch dann erreichen, wenn aggregierte und so anonymisierte oder zumindest pseudonymisierte Daten verarbeitet werden. Ist das der Fall, darf der Personenbezug insofern auch nicht erhalten bzw. – im Fall der Pseudonymisierung – offengelegt werden.

Werden personenbezogene Daten für die weitere Verwendung anonymisiert, so ist zu beachten, dass dies nach um-

strittener, aber wohl jedenfalls bei den Datenschutzaufsichtsbehörden noch vorherrschender Ansicht einer eigenen Erlaubnisgrundlage bedarf (siehe dazu BfDI, Positionspapier vom 19.6.2020).

Welche Anforderungen an die Anonymisierung und damit eine Beendigung der Anwendbarkeit des Datenschutzrechts gestellt werden, ist ebenfalls in der Diskussion. Nach der EuGH-Rechtsprechung zur früheren Datenschutz-Richtlinie, die in Erwägungsgrund 26 Satz 3-5 DSGVO ihren Niederschlag gefunden hat, wird eine absolute Anonymisierung nicht gefordert. Vielmehr sind Daten dann nach dem Verständnis der DSGVO anonym und unterliegen nicht (mehr) dem Anwendungsbereich des Datenschutzrechts, wenn unter Berücksichtigung der für den Verarbeiter zur Verfügung stehenden Mittel nach allgemeinem Ermessen eine Re-Identifikation wahrscheinlich nicht möglich ist. Dabei sind objektive Faktoren wie die Kosten und der Zeitaufwand einer Re-Identifikation zu berücksichtigen. Es ist mithin nicht – wie beim absoluten Ansatz – entscheidend, ob überhaupt eine Re-Identifizierung irgendwie denkbar bist. Vielmehr ist konkret zu prüfen, ob in dem Einzelfall eine Re-Identifizierung auch wahrscheinlich ist – oder ob sie nicht zu teuer und zu aufwändig wäre, als das ein realistisches Risiko besteht.

Bei einem Datenhandel mit nicht-personenbezogenen Daten ist das Datenschutzrecht nicht (mehr) anwendbar und muss folglich auch nicht eingehalten werden. Die weiteren regulatorischen Vorgaben – von DGA über DA hin zur Open-Data-Richtlinie oder auch dem ePrivacy-Recht bei Telemedienangeboten – gelten indes auch für nicht-personenbezogene Daten.

Datenquelle

Im nächsten Schritt ist als weitere rechtliche Vorfrage zu klären, woher die Daten, die genutzt, gehandelt, analysiert oder anderweitig monetarisiert werden sollen, stammen.

Im Fall personenbezogener Daten ist dies aufgrund des Zweckbindungsgrundsatzes nach Art. 5 Abs. 1 lit. b DSGVO entscheidend: Personenbezogene Daten dürfen regelmäßig nur für den Zweck verarbeitet werden, für den sie erhoben wurden. Eine Zweckänderung ist nur zulässig, wenn der neue Zweck mit dem bisherigen kompatibel ist i.S.d. Art. 6 Abs. 4 DSGVO und / oder (dies ist nach wie vor umstritten) es dafür eine gesonderte Erlaubnisnorm gibt. Sonderregelungen gibt es für eine privilegierte Weiterverarbeitung für Forschungszwecke oder für statistische Zwecke.

Die Weiterverwendung von Daten aus externen Quellen muss zudem etwaige (vertraglich vereinbarte) Nutzungsbeschränkungen beachten. Da eine gesetzliche Regelung zur Verfügungsgewalt fehlt, folgen diese regelmäßig aus den vertraglichen Abreden. Diese sind zu beachten, wenn Daten externer Herkunft zu anderen als den ursprünglichen Zwecken weiterverarbeitet werden sollen.

Ziele

Unternehmen sollten überdies bereits zu Beginn eines Projektes zum Datenhandel oder der anderweitigen Datenmonetarisierung oder -nutzung klar definieren, welche Ziele angestrebt werden. Diese Festlegung der Ziele ist elementar, um zu prüfen, ob die entsprechende Datenverarbeitung zulässig ist, mit Blick auf die Zweckbindung einer Verarbeitung personenbezogener Daten und auch etwaigen Nutzungsbeschränkungen.

Das Potential des Datenhandels ist vielfältig: Durch die Verwertung der Daten kann die Produktivität des Geschäfts optimiert werden, es können neue Geschäftsmodelle etabliert und damit weitere Einnahmequellen geschaffen oder auch eine bessere Kundenbindung erreicht werden. Unternehmen sollten daher ihre Ziele (frühzeitig) festlegen und ihre Strategie so anpassen, dass diese Ziele erreicht werden. Dies wirkt sich aus auf die Art und Weise der (strukturierten) Ablage der Daten, der Klassifizierungen und Risikoeinschätzungen sowie nicht zuletzt der Entscheidung, zu welchen Daten Zugang gewährt wird, zu Rohdaten oder etwa nur ausgewerteten, aggregierten Daten.

Rechtliche Anforderungen definieren

Im Dschungel der digitalen Regulierungen und tradierten Rechtsbereiche sind sodann die Regeln zu identifizieren, die für den geplanten Anwendungsfall des Datenhandels einschlägig sind. Neben der Frage, ob das Datenschutzrecht beachtet werden muss, sind dies insbesondere die folgenden Anforderungen:

- Nutzungsrechte: Es ist zu klären, wie mit den Daten umgegangen werden kann. Innerhalb welcher Grenzen sind diese lizenziert, was darf mit ihnen geschehen? Wenn Daten öffentlicher Stellen weiterverwendet werden sollen, so sind die öffentlichen Stellen nicht frei in den von ihnen ausgesprochenen Nutzungsbeschränkungen. Die Open Data-Richtlinie und der DGA sehen vielmehr vor, dass es nur geringe Weiterverwendungsbeschränkungen geben darf (und diese stets diskriminierungsfrei angewandt werden). Sollen Daten aus digitalen Verbraucherprodukten weiterverwendet werden, so sind auch für nicht-personenbezogene Daten gesetzliche Grenzen in § 327p BGB vorgesehen, die einzuhalten sind. Zudem ist zu klären, wie der Geschäftspartner mit den Daten umgehen darf: Welche Nutzungsrechte werden ihm eingeräumt, werden Daten auf

Dauer oder nur für eine begrenzte Zeit zur Verfügung gestellt, wie erfolgt die Bereitstellung?

- Künftig Absicherung von Zugangsrechten, Portabilität und Bereitstellung: Nach dem im Entwurf vorliegenden DA müssen Daten portabel sein, Nutzern ist Zugang auch zu Metadaten (Nutzungsdaten in Rohform) zu geben, was bei der Produktgestaltung zu beachten ist.
- Bei besonderen Diensten wie Datenmittlern oder alturistischen Datenorganisationen sind die engen Vorgaben des DGA zu beachten, um die dort vorgesehenen Privilegien nicht zu verlieren. U.a. ist über die Weiterverwendung von Daten umfassend zu informieren.
- Data Governance Principles: Jenseits des DGA und der harten rechtlichen Vorgaben ist schließlich zu empfehlen Prinzipien festzulegen, wie mit Daten im Unternehmen und bei den Geschäftspartnern umgegangen werden darf. Gibt es ethische Vorgaben, die wichtig sind?

Vertrag gestalten

Auf Basis der identifizierten rechtlichen Vorgaben ist sodann das Vertragswerk zu gestalten, welches den Datenhandel regelt. Mangels konkreter rechtlicher Vorgaben zu den Kernfragen der Leistungsdefinition, Datenbereitstellung und Verfügungsgewalt sowie Gewährleistung ist es von elementarer Bedeutung diesen Vertrag umfassend und solide auszuarbeiten. Anders, als in klassischen Bereichen wie dem Kaufrecht für körperliche Gegenstände oder der Raummiete fehlt es an gesetzlichen Regelungen, auf die im Zweifel zurückgegriffen werden kann.

Je nach Geschäftsmodell muss zunächst entschieden werden, ob ein Standardvertrag erstellt wird oder Individuallösungen für jeden einzelnen Vertragspartner ausgearbeitet werden. Wichtig ist in jedem Fall, dass eine exakte Leistungsbeschreibung mit der Art und Dauer der Datenverwertung sowie Angaben zur Datenqualität aufgenommen werden. Auch müssen nähere Angaben zur Bereitstellung, zu den Nutzungsrechten, insbesondere die ggf. erwünschte Begrenzung auf bestimmte Zwecke sowie zeitliche und räumliche Beschränkungen und zur Gewährleistung aufgenommen werden. Schließlich sind stets Aspekte wie die Vergütung und Haftung sowie Datenschutz und Datensicherheit – letzteres auch für nicht-personenbezogene Daten – zu regeln.

Über die Autorin

Dr. Kristina Schreiber
ist Fachanwältin für Verwaltungsrecht und Partnerin bei Loschelder Rechtsanwälte in Köln. Sie ist spezialisiert auf die rechtliche Begleitung von Digitalisierungsprojekten, von der App über individuelle Softwareprojekte bis hin zu Datennutzungsstrategien. Kristina Schreiber bloggt auf www.digitalisierungsrecht.eu. Sie ist unter anderem Herausgeberin des Praxisleitfadens „Digitale Angebote" und kommentiert zum TTDSG. Ein Einführungsband zum Data Governance Act, den sie mit verfasst hat, erscheint demnächst.

Anzeige

Für interne & externe Datenschutzbeauftragte

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

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

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

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

NEU:

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

BUTZ
VERSICHERUNGSMAKLER GMBH

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

DR. LUTZ HASSE, RENÉ RÖSEL

(THÜRINGER) SCHULEN: DIGITALISIERUNG UND MEDIENKOMPETENZ – WO KLEMMT'S?

1. Ausgangslage

Das Thema Digitalisierung der Schulen ist in aller Munde. Alle Bildungseinrichtungen wurden spätestens mit dem Aufkommen der Corona-Pandemie seit Anfang 2020 bei der Gestaltung des Unterrichts mit der Einführung digitaler Werkzeuge konfrontiert. Aufgrund der Schulschließungen und dem damit einhergehenden Ausfall des Präsenzunterrichts wurde flächendeckend Distanzunterricht eingeführt. Dies setzte zuallererst die digitale Kommunikation zwischen Schülerinnen und Schülern mit den Lehrkräften, aber auch der Lehrkräfte untereinander voraus. Um dieses auch künftig zu gewährleisten, müssen die Schüler:innen und die Lehrkräfte jeweils über ein Datenverarbeitungsgerät verfügen. Dabei werden heute eher weniger PCs genutzt, sondern fast ausschließlich ortsunabhängige mobile DV-Geräte wie Laptops, Tablets und Smartphones. Im Regelfall werden zur Durchführung des Online-Unterrichts Lernplattformen eingesetzt, die webbasiert auch Schüler- und Lehrerdaten verarbeiten. Lernplattformen können dann beliebig durch weitere Tools ergänzt werden. Hierzu zählen Videokonferenzsysteme oder Messenger-Dienste und darüber hinaus die zahllos auf dem Bildungsmarkt vorhandenen Angebote an Schulsoftwareprodukten. Da die Schule die genannten Produkte für Unterrichtszwecke einführt und damit über die Zwecke und Mittel der Verarbeitung der personenbezogenen Schüler- und Lehrerdaten entscheidet, ist jede Schulleitung „**Verantwortliche**" im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO). Damit ist nach Art. 5 Abs. 2, 24 Abs. 1 DS-GVO die Schule für die Einhaltung der DS-GVO verantwortlich und insoweit auch rechenschaftspflichtig. Die Schulleitung ist also nachweispflichtig, dass die personenbezogenen Daten datenschutzrechtskonform verarbeitet werden.

Sind die Schulen aber personell, technisch und finanziell für diese Anforderungen gerüstet? Und können medienkundliche Lehrinhalte an Schüler:innen weitergegeben werden? Wo hakt es noch und was muss unternommen werden, um Schulen leistungsfähiger zu machen? Diese Fragen beleuchtet der nachfolgende Artikel, basierend auf den Erfahrungen und Kenntnissen des TLfDI, der auch Bundesvorsitzender der Datenschutzkonferenz-Arbeitskreise Schulen und Bildungseinrichtungen sowie Datenschutz-/Medienkompetenz ist.

2. Digitalisierung an den Schulen

a. Grenzen des Digitalpakts

Aus der „Digitalstrategie Thüringer Schule – DiTS" ergibt sich unter anderem das Ziel, dass bis zum Ablauf des DigitalPakts Schule im Jahre 2024 für jede Schülerin und jeden Schüler ein durch digitale Medien und Technologien unterstütztes Lernen möglich ist.[1] Ein Baustein hierzu ist die Anschaffung von Datenverarbeitungsgeräten für die Schüler:innen. Die Entscheidung über die Anschaffung von schulgebundenen mobilen Endgeräten (Laptops, Notebooks, Tablets, **nicht** aber Smartphones) wird nicht von den Schulen, sondern von den Schulträgern vorgenommen. Die Schulträger beantragen beim zuständigen Ministerium die Gewährung von Zuwendungen in Form von Geldmitteln, etwa für den Aufbau oder die Verbesserung der Digitalen Vernetzung in der Schule einschließlich WLAN, Anzeige- und Interaktionsgeräte und schulgebundene mobile Endgeräte (Laptops, Notebooks, Tablets). Diese Mittel werden dabei überwiegend aus dem DigitalPakt Schule bereitgestellt. Dies ist in einer Verwaltungsvorschrift des Thüringer Ministeriums für Bildung, Jugend und Sport zur Umsetzung des DigitalPakts Schule 2019 bis 2024 vom 17.07.2019 geregelt.[2] Die mit diesen Geldern angeschafften Geräte, etwa Tablet-Klassensätze, werden von den Schulträgern an die Schulen ausgegeben. Im Regelfall übernimmt der Schulträger die Erstinstallation des Betriebssystems und weitere grundsätzliche Einstellungen. Die Verantwortung für die Zulässigkeit der

[1] https://bildung.thueringen.de/schule/medien/digitalpaktschule

[2] abrufbar unter: https://landesrecht.thueringen.de/bsth/document/VVTH-VVTH000009386

angeschafften Geräte sowie für die darauf gespeicherte Software inklusive eines Mobile Device Managements zur zentralen Wartung der Schülergeräte durch den Schulträger trägt grundsätzlich ebenfalls die Schule.

Auffällig ist, dass die finanziellen Mittel des Digitalpakts I nur recht verhalten abgerufen werden und schon der Digitalpakt II vor der Tür steht. Geld allein scheint also nicht das Allheilmittel zu sein. Ein Grund hierfür besteht darin, dass **baulich notwendige Maßnahmen** im Zusammenhang mit der Installation von Digitalisierungstechnik (zum Beispiel Durchbrüche, Kabelschächte, Technikräume) nicht aus Digitalpaktmitteln finanziert werden können und daher vom Schulträger zu tragen sind, was Digitalisierungsprojekte verzögern kann.

b. WLAN, BYOD, Support

Ein weiterer Grund dafür, dass der DigitalPakt Schule in den Bundesländern nicht die Wirkung zeigt, die er haben sollte, findet sich in der fehlenden oder unzureichenden Breitbandversorgung in den (Thüringer) Schulen. Hierzu passt auch ein Artikel der Thüringer Allgemeine vom 18.08.2022, der feststellt, dass das Bildungssystem von Thüringen im Bundesländervergleich auf Platz 3 klettert, bei der Digitalisierung der Schulen aber lediglich Platz 13 aller 16 Länder erreicht.[3] Ein damit einhergehendes nicht leistungsfähiges WLAN führt dann eben auch zur Unbrauchbarkeit der schönen Tablett-Klassensätze, wenn mehrere Schüler:innen damit arbeiten sollen. Bisweilen fehlt der Schulleitung schon das Wissen, wie es um den Internetanschluss ihrer Schule steht.

Solche Zahlen dürfen jedoch nicht darüber hinwegtäuschen, dass eine Geschwindigkeit von 51 bis 100 Mbit/s kaum ausreichen dürfte, eine Schule mit Blick auf Videodatenströme, Streaming oder Surfen ausreichend auszustatten.

Wie oben beschrieben erfolgt in den Thüringer Schulen die Anschaffung von schulgebundenen mobilen Endgeräten insbesondere aus Mitteln des DigitalPakts Schule. Die Gelder werden aber nicht ausreichen, um jedem Schüler in Thüringen ein eigenes Gerät zur Verfügung zu stellen. Daher bilden sich auf Initiative von Lehrkräften oder Eltern in vielen Schulen auch ohne die Bereitstellung solcher geförderten Endgeräte sogenannte „Tablet-Klassen".

Hierbei werden die Geräte in der Regel von den Eltern der Schüler:innen **selbst finanziert.** Teilweise hat sich der Elektronikhandel darauf eingerichtet und bietet bei der Abnahme eines gesamten Klassensatzes Schulkonditionen und Ratenzahlung an. Die Geräte stehen dann im Eigentum der Schüler:innen beziehungsweise deren Eltern. Es handelt sich also um **private** Endgeräte, die zu schulischen Zwecken eingesetzt werden, in jedem Fall aber **auch privat** Verwendung finden, sofern sie nicht in der Schule unter Verschluss genommen werden. Aus der Sicht des TLfDI ergeben sich aus solchen **BYOD (Bring Your Own Device)**-Lösungen zahlreiche datenschutzrechtliche Probleme.

Das Schulrecht enthält für diese Fälle keine speziellen Vorschriften. Es beginnt damit, dass die Geräte natürlich nur mit der **freiwilligen** Entscheidung der Eltern angeschafft und schulisch genutzt werden können. Die Nutzung erfolgt meist in Form einer digitalen Schulplattform, in Thüringen ist dies zu großen Teilen die Thüringer Schulcloud, zu kleineren Anteilen Moodle und weitere Lernplattformen, die über eine Webanwendung betrieben werden.

Zusätzlich wird auf Empfehlung einer Schule Software für schulische Anwendungen auf dem Gerät selbst installiert, die entweder Inhalt (Content) oder das Werkzeug (Tools) darstellen. Grundsätzlich muss die Schule jede Anwendung, die auf dem privaten Endgerät installiert ist und für schulische Zwecke genutzt werden soll, dahingehend prüfen, ob die Anwendung datenschutzkonform ist. Beispielsweise darf es **nicht zu datenschutzrelevanten Interaktionen zwischen privaten und schulischen Apps kommen**. Zusätzlich muss zur Trennung von schulisch veranlasster und privater Nutzung eine **Mobile Device Ma-**

Die Internetgeschwindigkeit an Thüringens Schulen

Schulen nach Geografie sowie Internetanschlussart (120)

mit Adressangaben

nach Anschlussart | nach Geschwindigkeit

nach Geschwindigkeit

Schuljahr:	21/22
Schulträger:	Σ
Schultyp:	Σ
Schulart:	Σ
EDV Einsatzbereich:	Schülerbereich
Measures:	Schulen

Geografie	Geschwindigkeit in Mbit/s								
Schulnummer	Σ	kein	1 bis 6	7 bis 16	17 bis 25	26 bis 50	51 bis 100	101 bis 250	über 250
Thüringen	933	6	30	171	25	96	238	249	118
Mittelthüringen	178	2	9	16	2	21	51	57	20
Nordthüringen	176	1	2	10	5	22	69	38	29
Ostthüringen	239		8	20	8	15	56	81	51
Südthüringen	165	3	4	65	2	15	35	32	9
Westthüringen	175		7	60	8	23	27	41	9

Schuljahresstatistik Schulen-Klassen-Schüler ABS ST+FT, Schuljahr: 21/22, Stichtag: 22.09.2021
Schuljahresstatistik Schulen-Klassen-Schüler BBS ST+FT, Schuljahr: 21/22, Stichtag: 10.11.2021

Quelle: Statistisches Informationssystem Bildung, Ministerium für Bildung, Jungend und Sport Freistaat Thüringen. https://www.schulstatistik-thueringen.de/

[3] vgl. „Thüringer Allgemeine" vom 18.08.2022 „Schwachstelle Digitalisierung"

nagement (MDM)-Software aufgespielt werden, um den schulischen Teil zu verwalten, also die Daten- und Gerätesicherheit zu prüfen, erforderliche Updates aufzuspielen oder die Einrichtung von starken Passwörtern oder eine Festplattenverschlüsselung zu erzwingen. Nachteil eines MDM ist, dass, je nachdem, welches Tablet verwendet wird, nicht nur auf den mit einer eigenen ID verwalteten schulischen Teil, sondern auch auf den privaten Teil zugegriffen werden kann. Mögliche Manipulationen können das Mitlesen eines Datenverkehrs oder das Tracking des Gerätes sein. Dies muss per Dienstanweisung ausgeschlossen werden. Nach bisherigen Erkenntnissen des TLfDI ist eine technische Verhinderung solcher Zugriffe schwer umzusetzen. Beispielsweise können auf iPad-Geräten keine separaten Containerbereiche eingerichtet werden. Zudem gibt es einige **schulrechtliche Vorschriften**, die die **Lehrkräfte** und die Schulleitungen zu beachten haben. So wird gemäß § 57 Abs. 8 Nr. 5 Thüringer Schulgesetz das Verarbeiten von personenbezogenen Daten der Schüler durch den Lehrer auf dessen Datenverarbeitungsgeräten außerhalb der Schule durch Rechtsverordnung geregelt. § 136 Abs. 6 Thüringer Schulordnung gibt vor, dass Lehrer, die bei der automatisierten Verarbeitung personenbezogener Daten von Schülern andere als vom Schulträger zu diesem Zweck zur Verfügung gestellte Datenverarbeitungsgeräte verwenden, durch **geeignete technische und organisatorische Maßnahmen** nach Artikel 24 in Verbindung mit Artikel 32 DS-GVO zu gewährleisten haben, dass dem Schutzbedarf der personenbezogenen Daten Rechnung getragen wird. Auf Verlangen des Schulleiters, eines Bediensteten der unteren Schulaufsichtsbehörde oder des Landesbeauftragten für den Datenschutz sind diese Sicherungsmaßnahmen **nachzuweisen**. Nach wie vor gültig ist in diesem Zusammenhang eine Verwaltungsvorschrift des damaligen Thüringer Kultusministeriums vom 5. Mai 2000[4]. Hiernach müssen die Lehrkräfte sich den Einsatz privater Rechner von der Schulleitung schriftlich genehmigen lassen und eine Verpflichtungserklärung unterschreiben. Es ist davon auszugehen, dass diese Verwaltungsvorschrift in vielen Schulen in Vergessenheit geraten ist.

Auf der jüngsten Veranstaltung des TLfDI im September 2022 zum Thema „Digitalisierung der Schule" wurde schließlich gefordert, dass ein **professioneller und nachhaltiger IT-Support durch Experten** gewährleistet sein muss, damit eine eingeleitete Digitalisierung nicht an fehlendem Support oder an fehlendem Support-Personal scheitert.

c. Zertifizierte Produkte

Nicht nur Schulen, sondern auch andere Behörden und insbesondere Unternehmen schreien geradezu nach datenschutzrechtlich zertifizierter Software, auf deren Datenschutzkonformität sich der Käufer und Nutzer verlassen darf. Warum gibt es die nicht?

Die Erklärung liegt darin, dass Art. 42 Abs. 1 DS-GVO nur Zertifizierungen von konkreten Datenverarbeitungs**vorgängen** erlaubt, fatalerweise **nicht** aber von Datenverarbeitungs**produkten**. Der dringend von Wirtschaft und Behörden gewünschte Zertifizierungsmotor für Softwareprodukte ist deshalb auch noch nicht angesprungen. Es gibt inzwischen einige Projekte, die Konzepte entwickeln, um zu einem der Datenschutzzertifizierung nach Artikel 42 DS-GVO ähnlichen Ergebnis für schulische Informationssysteme zu gelangen.

[4] Verarbeitung personenbezogener Daten von Schülern auf privaten Rechnern von Lehrkräften für dienstliche Zwecke", Verwaltungsvorschrift des TMBJS vom 05.05.2000, Az.: Z/Z5/02 803

Dies sind zum Beispiel das vom Bundesministerium für Bildung und Forschung geförderte **Projekt „DIRECTIONS“**[5] und das aus Mitteln des DigitalPakts Schule geförderte Projekt **„eduCheck“**.[6] Inzwischen haben die beiden Projekte eine fortlaufende Zusammenarbeit beschlossen. Der TLfDI ist Teil dieser Bestrebungen, allerdings ist ein zügiges Anspringen des Zertifizierungsmotors nicht zu erwarten.

d. Datenschutz

„Immer dieser lästige Datenschutz, der gerade in Krisenzeiten schnelle Lösungen verhindert“ – solche Sätze hört man leider oft und zumeist von Leuten, die die Bedeutung des Grundrechts der informationellen Selbstbestimmung noch immer nicht realisiert haben. Diese Leute mögen mit ihren Daten verfahren, wie es ihnen beliebt. Verstöße gegen das Datenschutz(grund)recht können gerade für Kinder fatale Folgen haben. Dabei sind **Kinderdaten** nach der DS-GVO besonders schützenswert. Jeder Datenkrümel im Netz wird eingesammelt und individualisiert ausgewertet (Profiling)[7] und solche Profile werden nicht nur für Werbezwecke eingesetzt. Um einen größtmöglichen Persönlichkeitsschutz zu gewährleisten, sind daher die Regelungen des Datenschutz- und des Datensicherheitsrecht gerade von Schulen dringend einzuhalten. Dass das nicht einfach ist, ist unstrittig:

Zum einen sind, wie eingangs unter 1. erwähnt, **Schulleitungen** für die Verarbeitung personenbezogener Daten von Kindern, Lehrer:innen, Eltern, Beschäftigten und Dritten datenschutzrechtlich verantwortlich. Ob hier die **Verantwortlichkeit** richtig adressiert ist, darf bezweifelt werden. Denn Schulleitungen können kraft ihrer Ausbildung zumeist nicht über ein umfangreiches Datenschutzwissen verfügen und sollten deshalb nicht für die Entscheidung über Zweck und Mittel der Datenverarbeitung haftbar gemacht werden.

Denn denkbar ist, dass man eine **gemeinsame Verantwortung von Schule und Schulträger nach Art. 26 DS-GVO** für die Verarbeitung annimmt, so dass beide Verantwortliche in einer Vereinbarung festlegen müssen, wer welche Verpflichtungen erfüllt. In Thüringen gibt es bislang aber keine Festlegungen, ob von einer gemeinsamen Verantwortung für die Verarbeitungen auszugehen ist. Deshalb wird derzeit von der Verantwortung der Thüringer Schulen für die Verarbeitung personenbezogener Daten mit der genannten Hard- und Software ausgegangen. Schließlich ist gut vorstellbar, dass die Auswahl von datenschutzrechtlich zulässigen Hard- und Softwareprodukten zur Nutzung in Schulen ausschließlich in der **Verantwortung des Thüringer Ministeriums** für Bildung, Jugend und Sport liegt. Dies würde die Schulen in diesem Bereich stark entlasten und für Rechtssicherheit sorgen[8]. Vor einiger Zeit hat **Berlin** genau diesen Schritt gemacht und die Verantwortlichkeit für die schulischen IT-Fachverfahren und die in Frage kommenden digitalen Lehr- und Lernmittel der zuständigen Senatsverwaltung zugewiesen (§§ 7 Abs. 2a, 64 Abs. 11 Schulgesetz Berlin).

Zum anderen ist die Entscheidung über den Einsatz von Schulsoftware alles andere als einfach, wie folgendes alltägliches Beispiel zeigt: Die Schulen setzen bisweilen neben landesweiten Schulclouds mit ihren Features selbständig weitere Schulsoftware für Unterrichtszwecke ein. Dies bedeutet, dass die Schule regelmäßig die Verarbeitung der personenbezogenen Schüler:innendaten bei einem Auftragsverarbeiter durchführen lässt. Die Schule Die Schule muss daher mit dem Softwarehersteller einen Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO abschließen.

Die im Internet angebotenen Schulsoftwareprodukte verarbeiten jedoch häufig die Daten auf Servern, die in Ländern außerhalb der EU oder des EWR stehen und in denen das Schutzniveau der DS-GVO nicht gegeben ist. Bei US-amerikanischen Unternehmen sind darüber hinaus Zugriffe durch US-amerikanische Behörden auf ausschließlich in der EU verarbeitete Daten nicht auszuschließen, wobei den betroffenen Personen kein wirksamer Rechtsbehelf zur Verfügung steht[9]. Der Europäische Gerichtshof hatte in seiner Entscheidung „Schrems II“ am 16. Juli 2020 den sogenannten Angemessenheitsbeschluss (Art. 45 Abs. 1 DS-GVO) der EU-Kommission, wonach das EU-US-Abkommen „Privacy Shield“ dem Datenschutzniveau der EU entsprechen soll, als Rechtsgrundlage für Datenübermittlungen in die USA für ungültig erklärt. Eine Datenverarbeitung durch einen solchen Auftragsverarbeiter wäre daher **grundsätzlich unzulässig.**

Eine weitere Problematik bei Anbietern von Schulsoftware betrifft die Tatsache, dass ein Abschluss eines **Auftragsverarbeitungsvertrags** mit der Schule bisweilen überhaupt **nicht vorgesehen** ist. Die Schule müsste dann - unter Verstoß gegen Art. 28 DS-GVO - den festgelegten Geschäftsbedingungen des Anbieters zustimmen. Die Nutzung einer solchen Software verstößt ebenfalls gegen die Bestimmungen der DS-GVO und ist somit unzulässig.

Ist eine Nutzung der Schulsoftware datenschutzrechtlich unzulässig, versuchen Schulen oder auch der Softwarehersteller teilweise eine **Einwilligung bei den Eltern** der Schüler:innen einzuholen, um die rechtswidrige Datenverarbeitung doch

[5] https://cii.aifb.kit.edu/deutsch/110_1121.php

[6] https://educheck.schule/

[7] https://www.tagesanzeiger.ch/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt-652492646668

[8] vgl. Bericht im MDR: Bildungsministerium fürchtet wegen Datenschutz bürokratisches Monstrum“, https://www.mdr.de/nachrichten/thueringen/homeschooling-datenschutz-unterricht-sicherheit-102.html

[9] Fisa 702, Cloud Act: https://www.bundestag.de/resource/blob/796102/ea53ffe8e08a9ab11e270719263d8c53/WD-3-181-20-pdf-data.pdf

noch zu legitimieren. Ein solcher Verstoß ist jedoch einerseits **gar nicht einwilligungsfähig**, da die hier verletzten Vorschriften nicht zur Disposition des Betroffenen stehen[10]. Schließlich scheitert eine **informierte Einwilligung** (vgl. Art. 4 Nr. 11 DS-GVO) für den nicht seltenen Fall, dass sich aus den Unterlagen des Auftragsverarbeiters ergibt, dass er **personenbezogene Daten (welche?) für eigene Zwecke (welche?)** nutzt, daran, dass mit Blick auf dieses Dunkelfeld nicht von einer Einwilligung gesprochen werden kann, die sich auf transparente Informationen des Auftragsverarbeiters stützen lässt und mithin **unwirksam** ist. Und selbst wenn sich der **Auftragsverarbeiter** hinsichtlich der Verarbeitung personenbezogener Daten für eigene Zwecke darauf berufen sollte, dass er insoweit nicht als Auftragsverarbeiter sondern **als Verantwortlicher** handele, so hilft ihm dies auch nicht, da er sich für solch intransparente Datenverarbeitung auf keine Rechtsgrundlage berufen kann. Lässt sich eine Schulleitung dennoch darauf ein, sind Verstöße gegen Art. 5 Abs. 2 (fehlender Nachweis der DS-GVO-Konformität), Art. 6 Abs. 1 (fehlende Rechtsgrundlage) und Art. 28 (fehlende Voraussetzungen für einen gültigen Auftragsdatenverarbeitungsvertrag) DS-GVO vorprogrammiert. Die Datenschutzkonferenz wird sich in Kürze hierzu äußern.

Videokonferenzen und YouTube

Videokonferenzsysteme sind erste Wahl im schulischen Distanzunterricht. Allerdings kann es auch hier zu einer unzulässigen Verarbeitung der Schüler- und Lehrerdaten kommen. Bei vielen Systemen kann nicht ausgeschlossen werden, dass während der Videokonferenz Inhalts- und Rahmendaten der teilnehmenden Personen an Dritte übertragen werden. Dies können die Bild- und Tondaten, der Hintergrund der Teilnehmenden sowie Metadaten der Sitzung (wo, wie lange, wie oft, wie viel Teilnehmer usw.) sein. Aus diesem Grund ist mindestens eine Transportverschlüsselung, besser noch eine Ende-zu-Ende-Verschlüsselung der Übertragung zu fordern. Ebenfalls muss gewährleistet sein, dass nur hierzu berechtigte Personen an der Videokonferenz teilnehmen (Nutzerauthentifizierung) und dass grundsätzlich keine Aufzeichnung der Sitzung erfolgt.[11] Zudem gilt das zuvor zur Auftragsverarbeitung Gesagte, sodass auf DS-Konformität der Datenverarbeitung des Auftragsverbeiters zu achten ist.[12]

Schließlich ist ein Augenmerk auf die Nutzung von **YouTube-Videos** im Unterricht zu legen und warum dies nicht in allen Fällen erlaubt ist. Hierzu muss man wissen, dass YouTube ein Tochterunternehmen von Google ist und bei jedem Anklicken eines Clips die IP-Adresse, Standortdaten, welches Video angeklickt wurde und bestimmte Konfigurationen des anfragenden Endgeräts YouTube beziehungsweise Google bekannt werden. Falls der Nutzer ein Google-Nutzerkonto besitzt, werden auch diese Daten übertragen. Ebenfalls erfolgen mögliche Datentransfers außerhalb der EU ohne angemessenen Rechtsschutz. Sollen Clips im Unterricht gezeigt werden, so muss dies auf DV-Endgeräten erfolgen, die **nur der Schule**, aber keiner bestimmten Person zugeordnet sind. Das Aufgeben von Hausaufgaben etwa, bei der sich die Schüler:innen ein oder mehrere bestimmte YouTube-Videos ansehen sollen, ist damit aus datenschutzrechtlichen Gründen nicht zulässig. Die Verantwortung trägt wiederum die Schulleitung.

Ein noch etwas neues Feld eröffnet sich mit der **digitalen Lern-/Lehrsoftware**. Sofern hier personenbezogene Daten von Schüler:innen verarbeitet werden, darf dies natürlich nur DS-GVO-konform geschehen. Nicht fern liegt der Gedanke, dass hier möglicherweise ein klassenübergreifendes **Profiling** von Schüler:innen stattfindet, um das individuelle Lernen/Lehren optimieren zu können. Verantwortliche Schulleitungen sind gut beraten zu prüfen, ob sie eine **Rechtsgrundlage** für solche Datenverarbeitungen haben, ob eine **Einwilligung der Eltern informiert** ist, ob sie den **Informationspflichten** nach Art. 13 DS-GVO gegenüber den Eltern rechtskonform nachkommen können und ob die **Voraussetzungen des Art. 28 DS-GVO (Auftragsverarbeitung)** gegeben sind. Die oben erwähnten Arbeitskreise der Datenschutzkonferenz haben sich dieser Problematik angenommen. In diesem Zusammenhang wird das **VIDIS-Projekt** seine Bedeutung erlangen.[13] Mit VIDIS – dem Vermittlungsdienst für das digitale Identitätsmanagement in Schulen - sollen künftig Lehrkräfte und Schüler:innen auf digitale Bildungsangebote einfach und sicher mit nur einem bereits bestehenden Benutzerkonto ihres Landes- oder Schulportals zugreifen können.

Noch ein Wort zur Entscheidung des **OLG Karlsruhe** vom 07.09.2022 (Az. 15 Verg 8/22), die als Entlastung für Verant-

[10] vgl. Beschluss der Datenschutzkonferenz vom 24.11.2021 zur Möglichkeit der Nichtanwendung technischer und organisatorischer Maßnahmen nach Art. 32 DS-GVO auf ausdrückli-chen Wunsch betroffener Personen, unter: https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf

[11] vgl. auch: https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf und https://www.datenschutzkonferenz-online.de/media/oh/20201111_checkliste_oh_videokonferenzsysteme.pdf

[12] vgl. https://datenschutz.hessen.de/pressemitteilungen/mit-schutzma%c3%9fnahmen-ist-zoom-f%c3%bcr-lehrveranstaltungen-an-hessischen-hochschulen

[13] https://www.vidis.schule/

wortliche sogar im Schulbereich euphorisch gefeiert wird, weil danach öffentliche Auftraggeber darauf vertrauen können, wenn ihnen ein IT-Anbieter Datenschutzkompatibilität zusichert.[14] Das wäre wirklich nett: Ein IT-Anbieter (Hersteller, Auftragsverarbeiter) sagt, das eingesetzte Produkt sei datenschutzkonform und der Schulleiter darf darauf vertrauen; das wäre jedoch etwas zu einfach. Selbst wenn man davon ausgeht, dass eine gerichtliche Entscheidung zum **Vergaberecht** Einfluss auf das Datenschutzrecht haben sollte, so besagt das OLG Karlsruhe lediglich Folgendes: "Sie hat in diesem Zuge zugesichert, dass personenbezogene Gesundheitsdaten ausschließlich an die (...) übermittelt werden und auch zu ihrer Verarbeitung die **EU nicht verlassen**, sondern nur in Deutschland verarbeitet werden." (juris Rn.34). Und sodann ein **wichtiger Vorbehalt** des OLG:

„Der öffentliche Auftraggeber darf ohne Widerspruch zu § 127 Abs. 4 Satz 1 GWB grundsätzlich davon ausgehen, dass ein Bieter seine vertraglichen Zusagen erfüllen wird.[15] Erst **wenn sich konkrete Anhaltspunkte** dafür ergeben, dass dies **zweifelhaft** ist, ist der öffentliche **Auftraggeber gehalten** durch Einholung ergänzender Informationen die Erfüllbarkeit des Leistungsversprechens beziehungsweise die hinreichende Leistungsfähigkeit des Bieters zu prüfen.[16] Danach müsste die datenschutzrechtlich verantwortliche Schulleitung also prüfen, **ob Daten die EU verlassen**. Weiterhin hätte sie bei **konkreten Anhaltspunkten zu prüfen**, ob das IT-Produkt datenschutzkonform personenbezogene Daten verarbeitet. Nun wissen wir, dass insbesondere amerikanische Produkte diese Vorgaben oft nicht erfüllen, wenn sich etwa aus ihren eigenen Unterlagen ergibt, dass sie **Daten in die USA übermitteln** oder sie dort offenlegen und dass sie überdies **personenbezogene Daten zu eigenen Zwecken verarbeiten. Diese Informationen**, die die Rechtswidrigkeit der Datenverarbeitung nach sich zögen (s. o.), sind verantwortlichen Schulleitungen unschwer zugänglich und stellen mithin **jene konkreten Anhaltspunkte** dar, die dem OLG Karlsruhe zufolge den **guten Glauben** an die Angaben des IT-Anbieters (Hersteller, Auftragsverarbeiter) eben **nicht schützen**. Mit der Folge, dass die **Schulleitung verantwortlich und haftbar bleibt**.

Interessierte Lehrer:innen, vielleicht auch Schulleitungen, die in der datenschutzrechtlichen Verantwortung stehen, sollten sich durch **juristische Märchen** nicht verblüffen lassen, sondern sich beispielsweise mit den bisher nicht entkräfteten

[14] https://www.news4teachers.de/2022/09/wegweisendes-urteil-behoerden-schulen-duerfen-darauf-vertrauen-wenn-it-anbieter-ihnen-datenschutz-kompatibilitaet-zusichern/

[15] OLG Düsseldorf, Beschluss vom 26.08.2018, Verg 23/18, juris Rn. 71; KG, Beschluss vom 21.11.2014, Verg 22/13, juris, Rn. 36

[16] OLG Düsseldorf, a.a.O.; KG, a.a.O.; OLG Frankfurt a.M., Beschluss vom 16.06.201, 11 Verg 3/15, juris, Rn. 82; OLG Brandenburg, Beschluss vom 20.11.2012, Verg W 10/12, juris Rn. 21; juris Rn. 29.

Argumenten des Landesbeauftragten für Datenschutz des Landes Baden-Württemberg auseinandersetzen[17] und den Argumenten der Datenschutzkonferenz.[18] Klar ist, dass Verantwortliche sehr schlecht beraten sind, wenn sie sich auf ein Urteil berufen sollten, dessen Voraussetzungen gar nicht vorliegen. Nach alledem dürfte nachvollziehbar sein, dass Schulleitungen nicht zugemutet werden kann in einfache datenschutzrechtliche Überlegungen, wie zuvor geschildert, einzutreten. Die datenschutzrechtliche Verantwortlichkeit muss daher anderenorts adressiert werden.

3. Medienkompetenz

a. Lehrpläne für die digitale Welt

Wenn es stimmt, dass Schüler:innen nicht für die Schule, sondern für das Leben lernen, stellt sich die Frage, ob die Schulen auch für das digitale Leben ausbilden. Sei es integrativ in allen geeigneten Fächern, sei es in einem eigenen Fach, etwa Medienkunde. Hierbei geht es nicht nur darum zu vermitteln wie ein Whiteboard funktioniert. Vielmehr muss es darum gehen, dass Schüler:innen lernen können, welche Chancen die digitale Welt bietet, aber auch, welche Gefahren dort lauern: Was macht mein Smartphone mit personenbezogenen Daten? Wie erkenne ich das und wie kann ich das unterbinden? Werden IT-Inhalte vermittelt, sodass Schüler:innen einfache Algorithmen berechnen können? Was ist KI?

Die Kultusministerkonferenz denkt erfreulicherweise politisch in diese Richtung. Ob allerdings die Lehrpläne die digitale Welt abbilden, sehen viele Schulleiter:innen kritisch.[19]

Erstaunlich ist vor diesem Hintergrund, wie selten in einer sich rasant verändernden digitalen Welt Lehrpläne angepasst werden. Wichtig erscheint jedenfalls, dass digitale Unterrichtsinhalte verpflichtend und prüfungsrelevant sind. Das setzt voraus, dass solche Unterrichtsinhalte überhaupt vermittelt werden können. Leider bestätigen Stimmen aus der Schülerschaft bisweilen, dass es im Fach Medienkunde alles andere als rund läuft.

Dem TLfDI vorgetragenen Einwänden, dass neue Unterrichtsinhalte oder gar ein neues Fach Medienkunde dazu führe, dass alte Unterrichtsinhalte wegfallen müssten, sollte in einer sich rasch wandelnden Welt keine durchschlagende Gewichtung beigemessen werden. Das Bessere ist nun einmal der Feind des Guten.

b. Die Aus-/Fortbildung von Lehrkräften

Selbstverständlich braucht man zur Vermittlung von Medienkompetenz, IT-Inhalten und Datenschutz in den Schulen kompetente Lehrkräfte. Allerdings stellt sich die Frage, wer diese Lehrkräfte hierfür sowohl aus- als auch fortbildet. Als unabdingbar erscheint es, dass die **Universitäten** den Lehramtsstudierenden hier unbedingt entsprechendes prüfungsrelevantes Wissen vermitteln. Vorstellbar wäre etwa, dass Lehramtsstudierende eine Datenschutzvorlesung an der Juristischen Fakultät besuchen und dort eine Klausur bestreiten, mit der sie Credit-Points sammeln können. Ebenfalls müssen im Vorbereitungsdienst an den Staatlichen Studienseminaren die Lehramtskandidat:innen zur Vermittlung von Medienkompetenz und Datenschutz (Privatsphärenschutz) angehalten werden. Insgesamt müssten auch hier die Lehr- und Bildungspläne angepasst werden. Bürokratischer Aufwand darf hier kein Hindernis sein. Der TLfDI unterbreitet bereits entsprechende Angebote für Lehramtsstudierende. Insgesamt erscheint das **universitäre Engagement jedoch noch recht verhalten.**

Als recht erfolgreich indes haben sich regelmäßige **Videokonferenzen und Schulleiterbriefe** des TLfDI erwiesen. Mit diesen Mitteln werden alle Schulleitungen zu grundsätzlichen und speziellen sowie aktuellen Fragen des Schuldatenschutzrechts und solchen zu **Schulsoftware** unterrichtet. Auch **FAQ-Kataloge** zum Schuldatenschutz helfen weiter.[20]

In Sachen Fortbildung leistet beispielsweise das Thüringer Institut für Lehrerfortbildung, Lehrplanentwicklung und Medien gute Arbeit; der TLfDI kooperiert.

Fortbildung setzt allerdings entsprechende **Zeitkontingente** und auch Fortbildungsfreude voraus. Entsprechende Planungen und Anreizsysteme sind hierfür notwendig.

c. Externes Expertenwissen

Lücken in der Vermittlung digitaler Unterrichtsinhalte könnten zum Teil und vorübergehend mit externem Expertenwissen geschlossen werden. Sicherlich verfügen **IT-ler oder Juristen** in der Regel nicht über pädagogische Qualifikationen. Allerdings ist ein solcher Externen-Unterricht besser als gar kein Unterricht. Viele Externe sind bereit, ehrenamtlich oder gegen eine Aufwandsentschädigung in den Schulen zu arbeiten. Dennoch bleibt dieser Weg oft verschlossen. Entscheider erscheinen hier einfach zu unflexibel.

[17] https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf

[18] TOP 9 und Anhang: https://www.datenschutzkonferenz-online.de/media/pr/20201030_protokoll_3_zwischenkonferenz.pdf

[19] vgl. „Spiegel"-Bericht: https://www.spiegel.de/panorama/bildung/deutschlands-schulleitungen-halten-stundenplaene-fuer-nicht-mehr-zeitgemaess-a-1f0f63f0-445d-4d57-8bd6-ff9a9d07fece

[20] https://bildung.thueringen.de/schule/medien/datenschutz-in-schulen

Oder den Schulen sollten entsprechende finanzielle Befugnisse an die Hand gegeben werden.

Die Einstellung von Medienpädagog:innen stellt sich als weiteres Problem dar, obwohl diese an den Schulen ein breites und wichtiges Betätigungsfeld haben. Informationen des TLfDI zufolge wissen **Medienpädagog:innen** oft nicht, was sie an den Schulen zuerst und zuletzt machen sollen, so gefragt sind sie.

Der TLfDI agiert ebenso wie die anderen Landesdatenschutzbeauftragten und der BvD mit seiner Initative „Datenschutz geht zur Schule" ein wenig als Externer, etwa indem er ein Video zum Thema „Drohne" für den Unterricht anbietet[21] mit vielen Angeboten anderer Datenschutzbeauftragter und Dritter. Ein Video des TLfDI zum Thema Smartphone wird in Kürze erscheinen.

d. Eigenes Fach digitale Medienkunde?

Der TLfDI mischt sich in die pädagogische Diskussion nicht ein, ob digitale Unterrichtsinhalte fächerübergreifend (integrativ) oder in einem eigenen Fach vermittelt werden sollen. Vielleicht könnten digitale Unterrichtsinhalte ja fächerübergreifend (integrativ) und in einem eigenen Fach den Schüler:innen angeboten werden, wobei sich das eigene Fach dann auf IT- und juristische Inhalte fokussieren könnte. Mit diesen Fragen haben sich in einem in Thüringen Aufsehen erregenden Gutachten Prof. Dr. Jens Wolling und Priscila Berger von der TU Ilmenau auseinandergesetzt.[22]

FAZIT

Den Autoren ist klar, dass sie sich als Nicht-Pädagogen auf vermintes Gelände begeben. Dennoch erschien es uns notwendig, einiges aus unserem täglichen Erleben zu veröffentlichen, um die Diskussion über die vielfachen Missstände im Schulbereich lebendig zu halten. Dabei ist uns unsere selektive Datenschutz-Wahrnehmung und die Unvollständigkeit des Gesagten bewusst. Schule leidet noch an vielen weiteren, hier ungenannten Defiziten. Trotzdem wollen wir die uns offenkundigen Missstände ansprechen, um vielleicht partielle Diskussionen oder gar Änderungen anzustoßen. Also scheuen Sie sich bitte nicht, Kritik zu üben oder bessere Vorschläge zu machen. Möglicherweise lassen sich mittels des Vehikels „Datenschutz" auch andere Fortschritte transportieren. Wir unterstützen Sie wirklich gern und in jeder Hinsicht, wenn ein auch nur kleiner Bezug zum Datenschutz oder besser (aber nicht ganz identisch) zum Schutz der Privatsphäre besteht. Laden Sie uns ein oder kommen Sie zu uns – wir sind für weitere Vernetzungen dankbar und bieten auch unsere Netzwerke gern der Koalition der Willigen an.

Erwähnenswert für Thüringen ist, dass ein behördlicher Datenschutzbeauftragter an jeder Schule und nicht, wie bisher, nur in jedem Schulamt, dem Datenschutz dienlich wäre. Da behördliche Datenschutzbeauftragte nicht auf den Bäumen wachsen, bietet der TLfDI gern an, sich an deren Ausbildung zu beteiligen.

Nicht unerwähnt soll bleiben, dass einige Datenschutz-Probleme im Schulbereich gelöst wären, wenn man sich von fragwürdiger Software trennen würde. Baden-Württemberg ist diesen Weg gegangen.[23] Andere Aufsichtsbehörden sind inzwischen gefolgt. Die Datenschutzkonferenz wird sich in Kürze hierzu abschließend äußern. Weitergehend und visionär hat sich der Thüringische Finanzstaatssekretär und CIO Dr. Hartmut Schubert geäußert: Er will künftig landesweit auf Open-Source-Produkte abstellen.[24]

Über die Autoren

Dr. Lutz Hasse (TLfDI)
legte die Juristischen Staatsexamina in Niedersachsen ab. Die Promotion erfolgte an der Universität Osnabrück während der „Jenenser Assistenz-Phase" an der Friedrich-Schiller-Universität Jena. Nach Aufenthalten in leitenden Positionen in verschiedenen Ministerien und beim Landesdatenschutzbeauftragten ist er seit 2012 der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit.

René Rösel
ist stellvertretender Referatsleiter beim TLfDI.

[21] https://www.datenschutz-leicht-erklaert.de/. Hingewiesen sei in diesem Zusammenhang auch auf die Seiten Youngdata, https://www.youngdata.de/ und klicksafe https://www.klicksafe.de/.

[22] https://www.db-thueringen.de/servlets/MCRFileNodeServlet/dbt_derivate_00041138/ilm1-2018100036.pdf

[23] https://www.swr.de/swraktuell/baden-wuerttemberg/im-neuen-schuljahr-keine-microsoft-office-produkte-mehr-an-schulen-in-bw-100.html; https://fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1/626585/anhang/2021-04-23_Empfehlung_LfDI.pdf

[24] https://www.thueringer-allgemeine.de/wirtschaft/land-verabschiedet-sich-von-windows-und-office-id235565913.html

JOHANNA KRIEGER

SOCIAL MEDIA UND ÖFFENTLICHE STELLEN:

Was ist beim Betrieb einer Fanpage zu beachten?

Nicht nur Unternehmen und Vereine, sondern auch öffentliche Stellen setzen für Informations- und Kommunikationsangebote inzwischen verstärkt auf soziale Netzwerke. Über diese Internet-Plattformen, die der Kommunikation, Interaktion und Präsentation ihrer Mitglieder dienen, soll auf die digitalisierte Welt eingegangen und ein breiteres, jüngeres Publikum erreicht werden. Viele öffentliche Stellen wie Ministerien, Kommunen oder Verwaltungsbehörden betreiben deshalb sogenannte Fanpages für den eigenen Auftritt in dem sozialen Netzwerk.

Grundsätzlich ist wohl was dran an dem Bedürfnis der öffentlichen Stellen, die Bürger:innen über alle verfügbaren Kanäle mit relevanten Neuigkeiten und Informationen aus der Welt der Verwaltung zu versorgen. Datenschutzrechtlich gilt es dabei jedoch einiges zu beachten. Denn während die öffentlichen Stellen ihre Informationen über die Plattformen bequem und schnell veröffentlichen können, werden bei der Einbindung der Inhalte in der Regel personenbezogene Daten der Besucher:innen wie IP-Adresse oder Cookies an die Plattformbetreibenden und an Drittanbieter (beispielsweise Partnerunternehmen des kommerziellen Plattformanbieters) übermittelt. Und zwar sowohl von den Besucher:innen, die bei der Plattform des sozialen Netzwerks registriert sind, als auch von den nicht registrierten. Dies geschieht über die sogenannte „Insights-Funktion", mittels derer personenbezogene Daten der Besucher:innen zur Erstellung von Nutzerprofilen, Seitenstatistiken über die Nutzung von Fanpages und zu Werbezwecken genutzt werden.
In verschiedener Rechtsprechung (insbesondere Rs. C-40/17 „*Fashion ID*" und C-210/16 „*Wirtschaftsakademie*") hat der Europäische Gerichtshof inzwischen ausdrücklich festgestellt, dass die Stellen, die einen eigenen Auftritt auf sozialen Netzwerken betreiben, für das Erheben personenbezogener Daten und deren Weiterleitung durch Übermittlung an Drittanbieter in der Regel mit den Plattformbetreibenden gemeinsam verantwortlich im Sinne von Artikel 26 der europäischen Datenschutz-Grundverordnung (DS-GVO) sind. Dem folgten Urteile des Bundesverwaltungsgerichts (Az. 6 C 15.18) und des Oberverwaltungsgerichts Schleswig (Az. 4 LB 20/13).

Öffentliche Stellen müssen sich beim Betrieb einer Fanpage auf der Plattform eines sozialen Netzwerks daher bewusst sein, dass sie den Schutz betroffener Personen gerade im Bereich der sozialen Netzwerke dadurch sicherstellen müssen, dass die datenschutzrechtlichen Vorschriften konsequent eingehalten werden. Dies vor allem vor dem Hintergrund der Vielzahl und der möglichen Sensibilität der dort verarbeiteten personenbezogenen Daten.

Öffentliche Stellen müssen also die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Einhaltung der Grundsätze aus Artikel 5 Absatz 1 DS-GVO nachweisen. Sie unterliegen als (Mit-)Verantwortliche der Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO und insbesondere der Verpflichtung zum Setzen technisch-organisatorischer Maßnahmen im Sinne der Artikel 24, 25 und 32 DS-GVO. Zudem ist im Rahmen der gemeinsamen Verantwortlichkeit eine umfassende, für Betroffene transparente vertragliche Vereinbarung erforderlich (Artikel 26 Absatz 1 Satz 2 und Absatz 2 DS-GVO).

Dass diese Voraussetzungen in der Praxis kaum einzuhalten sind, wird in unserer Arbeit als Aufsichtsbehörde immer wieder ganz deutlich. Wenn wir öffentliche Stellen konsultieren und mit ihnen die Nutzung sozialer Netzwerke erörtern, zeigt sich, dass sie ihrer Nachweispflicht hinsichtlich der Rechtmäßigkeit der Datenverarbeitung in der Regel nicht nachkommen können und auch keine (hinreichende) Vereinbarung zur gemeinsamen Verantwortlichkeit nach Artikel 26 DS-GVO vorlegen können. Sie sind nicht in der Lage, die genauen Verarbeitungen, die mit dem Betrieb ihres Kanals auf dem sozialen Netzwerk einhergehen, zu benennen und können dementsprechend auch nicht die notwenige Transparenz den Betroffenen gegenüber herstellen. Dies auch angesichts dessen, dass die sozialen Netzwerke ihre Datenschutzrichtlinien und Datenverarbeitungen regelmäßig ändern oder ihr Angebot ausweiten.

Das macht auch das kürzlich veröffentlichte „Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook Fanpages" (Version 1)[1] der Datenschutzkonferenz

[1] https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf

der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ganz deutlich. Die DSK beleuchtet darin die datenschutzrelevanten Aspekte, die es bei dem Betrieb einer Facebook-Fanpage zu beachten gilt.[2] Und sie kommt zu einem eindeutigen Ergebnis: Da es an einer wirksamen Rechtsgrundlage und der erforderlichen Transparenz fehlt, ist die Datenverarbeitung, die bei dem Besuch einer Fanpage geschieht, mit der DS-GVO sowie dem TTDSG nicht vereinbar.

Die Einwilligung der Bürger:innen kann schon mangels hinreichender Informationen über die durchgeführten Datenverarbeitungen nicht wirksam eingeholt werden; und eine Ausnahme vom Einwilligungserfordernis besteht nicht. Auf das berechtigte Interesse können sich öffentliche Stellen nicht stützen. Artikel 6 Absatz 1 Satz 1 lit. f) DS-GVO ist laut Satz 2 ausdrücklich für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung nicht anwendbar. Gerade die Erfüllung ihrer Aufgaben ist ja aber die Argumentation der öffentlichen Stellen, warum sie soziale Netzwerke nutzen wollen. Vor allem lässt die bereits beschriebene mangelhafte Informationslage zu den einzelnen Verarbeitungen beim Betrieb einer Fanpage die für das berechtigte Interesse erforderliche umfangreiche Interessenabwägung nicht zu. Und auch wenn öffentliche Stellen soziale Netzwerke in der Regel für ihre Öffentlichkeitsarbeit nutzen, sodass eine Verarbeitung in Erfüllung einer öffentlichen Aufgabe in Betracht kommt, kann eine über die Öffentlichkeitsarbeit hinausgehende Auswertung der Daten der Bürger:innen nicht mehr von dieser Rechtsgrundlage gedeckt sein. Und: Ohne hinreichende Informationen auch keine rechtskonforme Vereinbarung über die gemeinsame Verantwortlichkeit, keine Erfüllung der Transparenzpflichten. Vom Problem des Drittstaatentransfers ganz zu schweigen.

Nun könnte man meinen, die allseits diskutierte Abschaltung der „Insights-Funktion" könnte die Lösung für all diese Probleme sein. Verantwortliche Stellen, privat wie öffentlich, führen immer wieder an, die Abschaltung der Insights – so sie denn möglich ist – befreie sie aus der gemeinsamen Verantwortlichkeit und damit aus den datenschutzrechtlichen Anforderungen in Bezug auf den Betrieb einer Fanpage. Und das lässt sich durchaus hören. Zwar könnte grundsätzlich argumentiert werden, die gemeinsame Bestimmung von Zwecken und Mitteln folge auch ohne die Verarbeitung von Insights bereits daraus, dass die öffentlichen Stellen durch den Betrieb der Fanpage und die verbundene Datenverarbeitung im eigenen Interesse die Reichweite gegenüber den Bürger:innen erhöhen und sich den Netzwerk-Effekt des sozialen Netzwerks zunutze machen, welches wiederum von den Nutzer:innen-Daten für das eigene Geschäftsmodell profitiert. Allerdings darf nicht übersehen werden, dass der Europäische Gerichtshof in seinem Urteil *Wirtschaftsakademie*[3] eben ganz entschieden auf die Parametrierung abstellt, sprich die den eigenen Zielen entsprechende Verarbeitung der vom sozialen Netzwerk ausgewerteten Daten durch dessen Einbindung. Und zwar im Rahmen der Verarbeitung der Insights. Ob die Verfügung einer Aufsichtsbehörde an eine öffentliche (oder auch private) Stelle, ihre Fanpage abzuschalten, trotz Deaktivierung der Insights-Funktion Bestand haben und dem Verhältnismäßigkeitsprinzip gerecht werden kann, bleibt demnach abzuwarten. Die Augen und Ohren des LfDI BW richten sich gespannt auf die zu erwartende Rechtsprechung.

Als Folge der hier dargestellten Problematik entschied sich bekanntermaßen der LfDI BW selbst bereits Anfang 2020 dazu, aus Twitter auszusteigen und seinen öffentlichen Account dort zu löschen. Das Zauberwort für den LfDI BW lautet: Alternativkanäle! Auf diese setzt er sowohl im eigenen Doing als auch in seiner Beratungspraxis. Entsprechend berät der LfDI BW die Landesregierung sowie sonstige öffentliche Stellen des Landes Baden-Württemberg zum Aufbau datenschutzkonformer Angebote in Alternative zu den kommerziellen sozialen Netzwerken. Datenschutzkonforme Kommunikationsplattformen wie Mastodon oder PeerTube ermöglichen einen regen digitalen Austausch mit den Menschen, ohne ihre Daten in die Hand kommerzieller Unternehmen zu geben. Und die Plattformen erfreuen sich aktuell über viele und immer mehr neue Nutzer:innen. Öffentliche Stellen müssen hier gemeinsam ein Zeichen setzen und mit gutem Beispiel vorangehen, den kommerziellen Anbietern entgegentreten, es besser machen. Sie müssen ihre staatlichen Informationen in einem ersten Schritt auch über alternative Kanäle zur Verfügung stellen.[4] Und je mehr öffentliche Stellen dies tun, desto mehr der wünschenswerten Reichweite erlangt die öffentliche Verwaltung über dezentrale soziale Netzwerke – ganz ohne Datenschutzproblematik.

Über die Autorin

Johanna Krieger (geb. Brüssel)
leitet die Stabsstelle für Deutsche und Europäische Zusammenarbeit beim Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. In dieser Funktion wirkt sie in verschiedenen Expert-Subgroups des europäischen Datenschutzausschusses (EDSA) mit, unter anderem zum Thema Social Media. Sie beteiligt sich zudem an der Ausarbeitung europäischer Leitlinien und hält regelmäßig Fachvorträge rund um das Thema DS-GVO.

[2] Es ist davon auszugehen, dass die in dem Kurzgutachten getroffenen Aussagen auch auf den Betrieb eines Kanals in anderen kommerziellen sozialen Netzwerken übertragbar sind.

[3] Rn. 33 ff.

[4] Brink/Henning, "Öffentliche Stellen: Raus aus Facebook, Twitter, TikTok!", https://netzpolitik.org/2022/oeffentliche-stellen-raus-aus-facebook-twitter-tiktok/

Foto: Stefan Krutsch

50 JAHRE DATENSCHUTZ IN HESSEN

Maria Christina Rost

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) **Prof. Dr. Alexander Roßnagel** hat im Oktober 2022 zwei Themen aufgegriffen, die von besonderer Bedeutung sind. Zum einen hat vor mehr als 50 Jahren im Jahr 1970 das Hessische Landesparlament mit dem ersten Hessischen Datenschutzgesetz (HDSG) zugleich das erste Datenschutzgesetz weltweit verabschiedet. Nachdem die geplanten Feierlichkeiten 2020 pandemiebedingt nicht stattfanden, wurden sie am 6. Oktober 2022 in einem Festakt nachgeholt.

Die Hessische Landtagspräsidentin **Astrid Wallmann** (CDU) stellte in der Eröffnung unter anderem fest, dass mit der Verabschiedung des ersten Datenschutzgesetzes weltweit der Hessische Landtag im Jahr 1970 internationale Datenschutzgeschichte geschrieben habe. Das Gesetz habe das Amt des Hessischen Beauftragten für Datenschutz als unabhängige Kontrollbehörde geschaffen. Wie wichtig und zukunftsweisend diese Entscheidung gewesen sei, zeige sich bis heute. Der Datenschutz stehe im digitalen Zeitalter vor ganz besonderen Herausforderungen. **Prof. Dr. Kristina Sinemus**, (CDU), Ministerin für digitale Strategie und Entwicklung in Hessen, gratulierte für die Landesregierung. Der Datenschutz habe mit zunehmender Digitalisierung noch mehr an Relevanz gewonnen. Gerade persönliche Daten wie im Gesundheitssektor seien ein höchst schützenswertes Gut. Daher brauche man eine gute Balance zwischen dem Nutzen der Daten und dem Schutz von Daten. Dann gelinge eine verantwortungsvolle Digitalisierung zum Wohle aller in der Gesellschaft.

Im Festvortrag würdigte **Prof. Dr. Thomas von Danwitz**, Richter am EuGH, die noch heute aktuellen Zielsetzungen und Vorgaben des ersten Hessischen Datenschutzgesetzes, die sich auch im europäischen Datenschutzrecht wiederfänden. Er skizzierte die Grundgedanken der Rechtsprechung des EuGH und schloss mit der Erkenntnis: „Eine demokratische Gesellschaft, die den Bürger ernst nimmt und – wie die Charta der Grundrechte – „den Menschen in den Mittelpunkt ihres Handelns“ stellt, verwirklicht sich im Zeitalter der Digitalisierung auch und vor allem durch einen hochwertigen Datenschutz. Dieser ermögliche dem Bürger Institutionen des Staates und Wirtschaftsunternehmen gleichermaßen in freier Selbstbestimmung auf Augenhöhe zu begegnen.“

Einen historischen Bogen spannte Prof. Dr. Alexander Roßnagel. Er erinnerte an die Bedingungen der Datenverarbeitung und des Datenschutzes vor 50 Jahren mit „Gebietsrechenzentren, Lochkarten und Magnetbändern“ und kontrastierte sie mit den heutigen Herausforderungen durch die Datenmacht globaler Internetkonzerne und weltweit vernetzter Datenverarbeitung. Er schloss mit der Feststellung: „Gerade angesichts dieser radikalen Veränderungen gilt noch immer die Zielsetzung des ersten Hessischen Datenschutzgesetzes, dass Freiheitsrechte und Demokratie die Einhegung der Informationstechnik voraussetzen. Nur wenn sie durch datenschutzrechtliche Leitplanken und datenschutzgerechte Technikgestaltung geschützt werden, können wir sicher sein, dass wir mit Informationstechnik besser leben als ohne sie.“[1]

[1] Festvortrag Prof Dr. von Danwitz: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Datenschutz%20in%20Hessen%20und%20Europa_6_10_22_von%20Danwitz_kV.pdf; Schlusswort Prof. Dr. Roßnagel: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Ro%C3%9Fnagel%20Vortrag%20Festakt%2050%20Jahre%20Datenschutz%20in%20Hessen.pdf

DATENSCHUTZ STÄRKT FORSCHUNG

Das 25. Wiesbadener Forum Datenschutz, das der HBDI nach zwei Jahren pandemiebdingter Pause am 6.10.2022 wieder im Hessischen Landtag durchführte, widmete sich dem Thema „Stärkung der Forschung durch Datenschutz". Forschung und Datenschutz werden vielfach als gegensätzliche Interessen gesehen. Forschungsfreiheit und informationelle Selbstbestimmung sind beides Grundrechte. Sie bedürfen einer Zuordnung, die das jeweils andere Grundrecht möglichst wenig einschränkt. Dann kann auch das Vertrauen der Patienten, die in die Verwendung ihrer Daten einwilligen sollen, gewonnen werden.

Festrede Prof. Dr. Thomas von Danwitz, Richter am EuG, Foto: Stefan Krutsch

Der BfDI **Prof. Ulrich Kelber** ging in seinem Vortrag „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" der Frage nach, welcher rechtspolitische Rahmen notwendig ist, um das Ziel verantwortungsvoller Datennutzung zu erreichen. Hierfür formulierte er zehn Gebote - zB die Unterstützung öffentlicher Interessen an der Forschung, die aktive Mitwirkung der betroffenen Personen, der Schutz personenbezogener Daten durch Anonymisierung, Pseudonymisierung und Verschlüsselung, den Einsatz von Datentreuhändern sowie den Schutz vor Re-Identifizierung.

In ihrem Vortrag „Der besondere Schutz der Forschung in der Datenschutz-Grundverordnung" untersuchte **Prof. Dr. Franziska Boehm** vom Karlsruher Institut für Technologie (KIT) welche besondere Berücksichtigung von Forschungsinteressen die DS-GVO vorsieht und wie diese Sonderregeln in der Praxis zur Anwendung kommen könnten. Dabei wies sie auf Ausnahmen z.B von der Zweckbindung, Datenminimierung, Speicherbegrenzung, Bestimmtheit der Einwilligung, Rechten der betroffenen Personen und Voraussetzungen der Datenübermittlung in Drittländer hin. Außerdem biete sie den Mitgliedstaaten Öffnungsklauseln, um Forschungszwecke weiter zu bevorzugen. Diese sollten genutzt werden, um auch im deutschen Recht unterschiedliche Rechtsregelungen zur Forschung zu harmonisieren.

Prof. Dr. Dr. Eric Hilgendorf von der Universität Würzburg berichtete in seinem Vortrag „Der Datenschutz in der künftigen Regulierung europäischer Forschungsdatenräume" von insgesamt 49 Gesetzgebungsakten oder -initiativen der Europäischen Kommission zur digitalen Transformation Europas. Zur Erleichterung der Datennutzung – insbesondere für Forschungszwecke – dienten vor allem der Data Governance Act und die Entwürfe für einen Data Act sowie zur Regulierung von insgesamt 13 europäischen Datenräumen. Dabei stellte er fest, dass der Datenschutz in diesen Gesetzgebungsakten keine systematische Berücksichtigung finde. Daher plädierte er für ein Moratorium, um Schutzvorkehrungen vor negativen Auswirkungen auf die Grundrechte ausreichend zu justieren.

Prof. Dr. Hannes Federrath von der Universität Hamburg zeigte in seinem Vortrag „Datenschutzwahrende Methoden der Forschungsdatenverarbeitung"auf, wie modernste Methoden der Informatik dazu beitragen können effektive Forschungsprozesse ohne Datenschutzprobleme zu ermöglichen. Als Schutzmöglichkeiten stellte er fünf Privacy-Design-Strategien vor: Minimize (Beschränkung auf notwendige Daten), Separate (dezentrale Datenauswertung am Speicherort), Aggregate (von Personenbezug abstrahieren), Pertubate (Personenbezug durch Verrauschen ausschließen) und Hide (Zugriff auf personenbezogene Daten verhindern).

Über die Autorin

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

▶ https://datenschutz.hessen.de/

PHILIPP OTTO, VERENA TILL

WIE KI VERTRAUENSWÜRDIG WIRD

Datenschutz als wesentlicher Faktor vertrauenswürdiger KI

Algorithmische Systeme und Künstliche Intelligenz (KI) sind nicht nur Begriffe aus Fachdiskussionen, sondern kommen vielfach und täglich zur Verwendung. Mit ihrer Hilfe werden Entscheidungen getroffen, die erhebliche Auswirkungen auf unser Leben haben.

Der Einsatz von KI-Anwendungen – beispielsweise in der Verwaltung, der medizinischen Versorgung, bei Navigationssystemen oder in den sozialen Medien – verspricht mitunter Erleichterungen im Alltag und verbesserte Dienstleistungen.

Doch wie werden KI-Anwendungen zum Wohle der Gesellschaft gestaltet und wie können eine menschenzentrierte Ausrichtung sowie das Vertrauen in die eingesetzten Technologien gestärkt werden? Mit diesen gesellschaftlich relevanten Fragen beschäftigt sich das Zentrum für vertrauenswürdige Künstliche Intelligenz (ZVKI) und leistet – unter Einbindung möglichst vieler Stakeholder*innen aus Wissenschaft, Wirtschaft, Politik und Zivilgesellschaft – einen wichtigen Beitrag zu deren Beantwortung.

Das Zentrum für vertrauenswürdige Künstliche Intelligenz (ZVKI)

Mit Unterstützung des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) baut der unabhängige Think Tank iRights.Lab, in Zusammenarbeit mit den Fraunhofer-Instituten AISEC und IAIS sowie der Freien Universität Berlin, das Zentrum auf. Das ZVKI soll als zentraler Ort der Debatte in Deutschland die Entwicklungen rund um gesellschaftliche Fragen zu Künstlicher Intelligenz und algorithmischen Systemen greifbar machen. Im Fokus des Projekts steht zudem die Gründung eines gemeinnützigen Vereins, der die Projektziele über die Förderungsphase hinaus weiterverfolgen soll.

Datenschutz – eine der richtigen Zutaten für vertrauenswürdige KI

Bezüglich des Einsatzes von KI-Anwendungen herrscht grundsätzlich eine eher positive Einstellung in der deutschen Bevölkerung. Viele Menschen befürchten jedoch, dass diese nicht zuverlässig genug sind, falsche Ergebnisse liefern können oder zu Manipulation und Massenüberwachung eingesetzt werden. Die meisten nachteiligen Entwicklungen werden bei Hacker-Angriffen auf persönliche Daten sowie deren Missbrauch mithilfe von KI gesehen. Zu diesen Ergebnissen kommt eine repräsentative Online-Befragung des ZVKI zu Vertrauen und Wissen über das Thema KI in der deutschen Bevölkerung.[1]

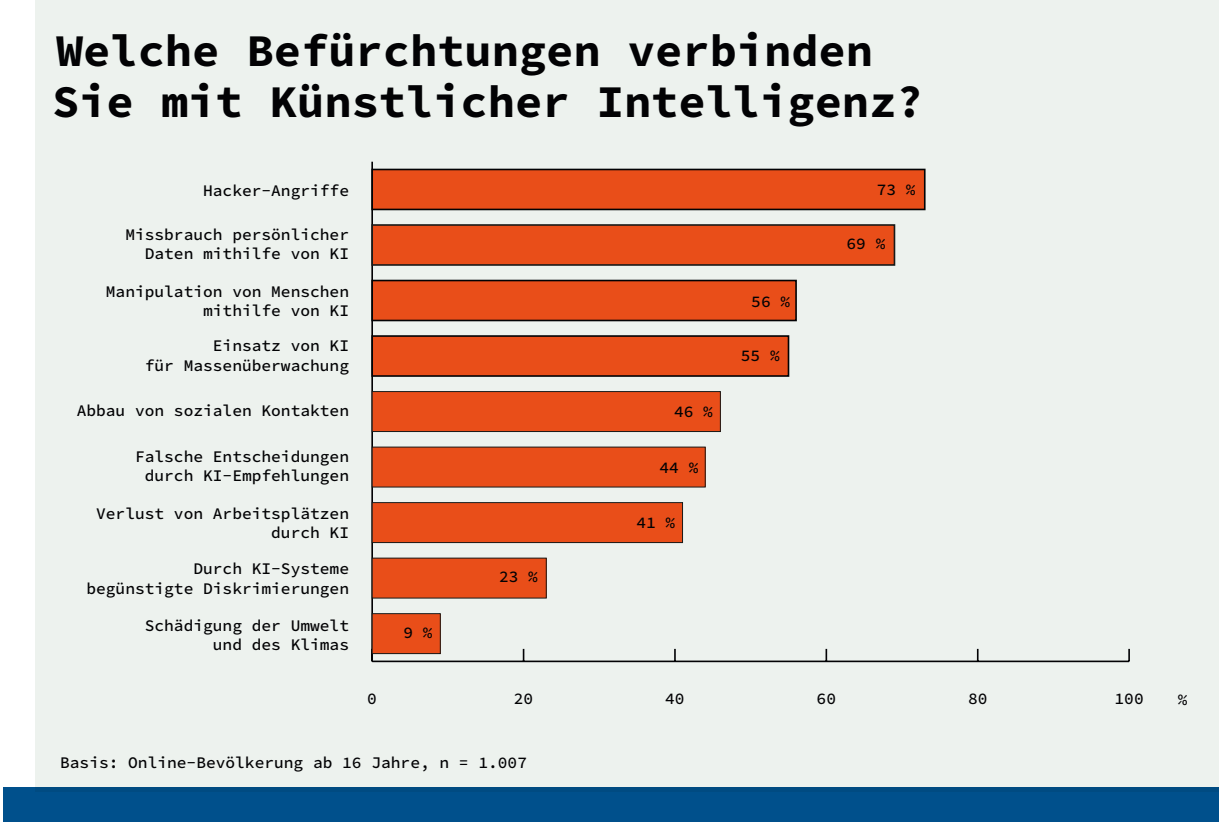
Die Befragten scheinen die Risiken von KI-Systemen zum einen auf eine etwaige unmittelbare Betroffenheit zu beziehen. Eine weitere mögliche Erklärung ist, dass IT-Sicherheit und Datenschutz im Vergleich zu anderen Aspekten in der Medienberichterstattung deutlich präsenter sind und von den Befragten deshalb eher genannt werden.

So überrascht es wenig, dass aus Sicht der Bürger*innen Datenschutz das wichtigste Kriterium für vertrauenswürdige KI-Systeme ist: 80 Prozent der Befragten erachten es als sehr wichtig, dass KI-Systeme Datenschutzanforderungen erfüllen.[2]

Der Schutz der Privatsphäre ist – nicht nur aus Sicht der Befragten – ein anerkanntes und breit diskutiertes Kriterium für ethische und vertrauenswürdige KI-Anwendungen. So formulierte bereits 2019 die von der Europäischen Kommission ernannte Hochrangige Expertengruppe für Künstliche

[1] Busse, Franziska; Baeva, Gergana: Was sind die richtigen Zutaten für vertrauenswürdige Künstliche Intelligenz? 2022. Online unter: https://www.zvki.de/zvki-exklusiv/fachinformationen/online-befragung (14.10.2022).

[2] Ebd.



Ergebnisse der ZVKI-Online-Befragung, die im Mai 2022 stattfand.

Intelligenz verschiedene Anforderungen an vertrauenswürdige KI.[3] Der Schutz personenbezogener Daten sowie die Sicherung von Datenqualität stellen demnach – neben technologischen Eigenschaften wie technischer Robustheit und Sicherheit sowie weiteren Kriterien wie Transparenz, Fairness und Vielfalt – wichtige Stellschrauben dar, um ethische Ansprüche an KI-Systeme zu bewerten.

Erst wenn KI-Systeme ethischen Standards genügen und Bürger*innen bestimmte Werte und Prinzipien wie Nachvollziehbarkeit, Gleichbehandlung oder den Schutz der Privatsphäre als erfüllt betrachten, werden sie diese Technologie auch als vertrauenswürdig ansehen. Um die Voraussetzungen für vertrauenswürdige KI zu schaffen, muss daher ein breiter öffentlicher Diskurs zu KI-Systemen und ethischen Werten angestoßen werden, der nicht nur Entscheidungsträger*innen aus Wirtschaft, Wissenschaft und Politik, sondern auch die Zivilgesellschaft einbezieht und ein bestimmtes Maß an (Grund-)Wissen vermittelt.[4] Um dem Informationsbedarf der Bevölkerung zu KI-Anwendungen zu begegnen und deren Vertrauenswürdigkeit zu fördern, stellt das ZVKI zielgruppenspezifische Inhalte und Formate bereit. Damit vermitteln wir den Bürger*innen Wissen zu Risiken und Chancen von KI-Systemen, um sie zu eigenständigem Handeln zu befähigen. Die Verantwortung für die Beurteilung eines KI-Systems hinsichtlich seiner Vertrauenswürdigkeit darf jedoch nicht auf die Verbraucher*innen abgewälzt werden. Vielmehr müssen Verfahren und technische Werkzeuge erforscht werden, die eine Überprüfung von KI entlang ethischer Prinzipien ermöglichen.

Grundlagenforschung des ZVKI im Bereich „vertrauenswürdige KI“

Der Datenschutz spielt bei komplexen Verfahren des maschinellen Lernens – einer grundlegenden Methode im Bereich Künstlicher Intelligenz – eine besondere Rolle, vor allem, da solche KI-Modelle zunehmend auch in sensiblen Bereichen wie der medizinischen Versorgung, bei Bewerbungsverfahren oder Finanzdienstleistungen eingesetzt werden.[5] Beim Machine Learning (ML) wird ein Modell mithilfe von sogenannten Trainingsdaten dahingehend optimiert Muster in Daten zu erkennen. Um auch bei zukünftigen Abfragen mit unbekannten Daten sinnvolle Ergebnisse zu produzieren, muss das Modell die Eigenschaften dieser Trainingsdaten „verinnerlichen“. Das Verfahren hinterlässt daher Spuren im Modell. Mittlerweile ist klar, dass diese Spuren keine anonymisierten Abstraktionen sind, sondern Rückschlüsse auf die ursprünglichen Trainingsdaten zulassen.

[3] High-Level Expert Group on AI: Ethics Guidelines for Trustworthy Artificial Intelligence. 2019. Hg. v. Publications Office of the EU. Online unter: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (14.10.2022).

[4] Müller-Brehm, Jaana: Wann beurteilen Nutzer*innen Künstliche Intelligenz (KI) als vertrauenswürdig? 2022. Online unter https://www.zvki.de/zvki-exklusiv/fachinformationen/nutzerinnenundvertrauen (14.10.2022).

[5] Boenisch, Franziska: Privatsphäre und Maschinelles Lernen. Über Gefahren und Schutzmaßnahmen. 2021. In: Datenschutz und Datensicherheit (45), S. 448-452, hier S. 448. Online unter: https://link.springer.com/content/pdf/10.1007/s11623-021-1469-3.pdf (14.10.2022).

Wesentliche Ziele des ZVKI: Information, Wissenschaft, Evaluation, Zertifizierung

Das ZVKI greift das Ziel Verbraucher*innen über Potenziale, Risiken und Anwendungsgebiete der KI-Technologie zu informieren, mit vielfältigen Formaten auf. Zudem analysieren wir Vorschläge der Regulierung, Evaluation und Zertifizierung von KI-Systemen, um möglichen Risiken zu begegnen. In unseren Facharbeitsgruppen betrachten wir Verfahren der Transparenz und der Nachvollziehbarkeit und leiten Empfehlungen ab, wie diese für Verbraucher*innen gestaltet werden sollen. Unsere Verbundpartner*innen – die Freie Universität Berlin sowie die Fraunhofer-Institute AISEC und IAIS – erforschen grundlegende Fragen des Datenschutzes, der Fairness und der Robustheit von KI-Systemen. Die Ergebnisse dieser Arbeit diskutieren wir mit Vertreter*innen aus Industrie, Wissenschaft und Zivilgesellschaft, um relevante Themen und Handlungsbedarfe im Bereich des Verbraucher*innenschutzes zu adressieren.

Gezielte Angriffe können daher einzelne Datenpunkte oder Dateneigenschaften wiedergewinnen und im schlimmsten Fall sensible Informationen über konkrete Personen offenbaren.[6]

Rund 30 Teilnehmende des zweiten ZVKI-Meetups der Reihe „Trustworthy Machine Learning Berlin" beschäftigten sich im August 2022 damit, welche datenschutzrechtlichen Herausforderungen das ML bereithält und wie Datenschutzrisiken begegnet werden kann.[7] Die regelmäßig stattfindenden Treffen zielen darauf ab Forscher*innen, Entwickler*innen und Nutzer*innen des maschinellen Lernens sowie Interessierte zum Austausch über Anforderungen für vertrauenswürdige KI und zur Vernetzung zusammenzubringen.

Einer der ZVKI-Verbundpartner*innen – die Freie Universität Berlin – arbeitet aus diesem Grund an Lösungen, die beides sicherstellen sollen: Maschinell lernende Modelle, die keine privaten Daten offenbaren und gleichzeitig präzise Ergebnisse liefern. Erfolg versprechend sind hierbei Ansätze der personalisierten Datenschutzniveaus, sodass Datenpunkte unterschiedlich stark verzerrt werden können. Ergänzend können kleinere Modelle separat trainiert und getrennt geschützt werden, sodass das finale Modell möglichst wenig an Präzision verliert. Experimente der Forschungsgruppe zeigen, dass solche Ansätze Datenschutz bei hoher Qualität der KI-Modelle garantieren können.[8] Großes Potenzial besitzen auch künstlich generierte Daten, die ein Trainieren von KI-Modellen ohne reale Daten erlauben würden. Bis solche Verfahren jedoch eingesetzt werden können, werden weitere Studien benötigt. In der Zwischenzeit lohnt es sich zu prüfen, wie der Einsatz sensibler Daten grundsätzlich minimiert werden kann. Zudem brauchen Unternehmen mehr Expertise, um datenschützende Verfahren effektiv einsetzen zu können.[9]

Fazit: Datenschutz ist zentraler Faktor für Vertrauen in KI-Systeme

Der Schutz der Privatsphäre hat bei KI-Anwendungen einen besonderen Stellenwert und ist deshalb eine der wesentlichen Anforderungen an die Vertrauenswürdigkeit der Technologie. Datenschutzfragen sind in diesem Kontext besonders brisant, da lernende KI-Systeme angreifbar sind. Machine-Learning-Modelle sind auf große Mengen oft personenbezogener Daten angewiesen. Bevor Verbraucher*innen eine KI-Anwendung überhaupt nutzen können, haben sie in vielen Fällen bereits mit ihren Daten zu deren Entwicklung beigetragen. Auch während des Betriebs müssen je nach Anwendung weitere personenbezogene Daten gesammelt und verarbeitet werden. Die Verarbeitung solcher Daten hinterlässt Spuren im trainierten Modell und lässt nachträglich Rückschlüsse auf sensible Daten zu. Die Sicherstellung umfassenden Datenschutzes ist daher eine zentrale Herausforderung bei Verfahren des maschinellen Lernens. Zurzeit werden technische Ansätze in der Wissenschaft intensiv erforscht und diskutiert. Die Entwicklung von Verfahren, die einen effektiven Datenschutz bei lernenden KI-Systemen sicherstellen, ist ein zentrales Forschungsfeld im Bereich KI, zu dem auch die Verbundpartner*innen des ZVKI einen wertvollen Beitrag leisten.

Datenschutzfragen rund um KI fordern uns auf den Verbraucher*innenbegriff neu zu denken und in allen seinen Facetten zu erfassen: Verbraucher*innen sind Datensubjekte, Nutzer*innen und Betroffene. Der Blick auf diese verschiedenen Verbraucher*innenrollen hilft konkrete Handlungsfelder zu umreißen und Handlungsbedarfe anzumelden. Beim Datenschutz sollten

[6] Ebd., S. 448ff.

[7] Schmechel, Lisa: Recap: Meetup #2 der Reihe „Trustworthy Machine Learning Berlin". 2022. Online unter https://www.zvki.de/aktuelles/recap-meetup-2 (14.10.2022).

[8] Boenisch, Franziska et al.: Individualized PATE: Differentially Private Machine Learning with Individual Privacy Guarantees. 2022. Online unter: https://arxiv.org/pdf/2202.10517.pdf (14.10.2022).

[9] Boenisch, 2021, S. 452.

folgende Fragen dringend beantwortet werden: Wie werden Datensätze erzeugt? Wie holen Hersteller*innen die Zustimmung der Verbraucher*innen ein? Wie können methodische Risiken bei Verfahren des maschinellen Lernens reduziert werden? Die Betrachtung der Verbraucher*innenrollen entlang solcher Fragen stellt eine wesentliche Aufgabe des ZVKI dar, um einen effektiven Verbraucher*innenschutz bei KI-Systemen auf die gesellschaftliche Agenda zu setzen.

ÜBER IRIGHTS.LAB

Das iRights.Lab ist ein unabhängiger, interdisziplinär ausgerichteter digitalpolitischer Think Tank in Deutschland, der sich besonders dem öffentlichen Interesse verpflichtet sieht. Kern der Arbeit des iRights.Lab ist die Entwicklung von Strategien und praktischen Lösungen, um die Veränderungen in der digitalen Welt vorteilhaft zu gestalten.

Über die Autor:innen

Philipp Otto
ist Gründer und Direktor des Think Tanks iRights.Lab. Seine Arbeitsschwerpunkte liegen in der strategischen Entwicklung von Strukturen, Konzepten und Modellen zur schnellen und konstruktiven Bewältigung von Herausforderungen, die durch die Digitalisierung für die Politik sowie öffentliche und private Einrichtungen entstehen. Er leitet das Projekt ZVKI.

Verena Till
ist im Team Forschung & Projekte beim iRights.Lab tätig und koordiniert das ZVKI. Zuvor hat sie viele Jahre in der Trend- und Zukunftsforschung gearbeitet. Ihr besonderes Interesse gilt Fragestellungen im Kontext einer zunehmend durch KI geprägten Welt.

▶ zvki.de

MITMACHEN!

Für Interessierte gibt es zahlreiche Möglichkeiten der Beteiligung. Daher sind Sie stets eingeladen, sich über verschiedene Wege zu beteiligen und einzubringen: Beschäftigen Sie sich mit unseren Inhalten zum Thema vertrauenswürdige Künstliche Intelligenz, beteiligen Sie sich an unseren ZVKI-Fach-AGs oder treffen Sie uns bei Veranstaltungen, an Stationen unserer Roadshow oder bei Vorträgen und Fachdiskussionen.

Weitere Informationen finden Sie auf unserer Webseite zvki.de.

Folgen Sie uns in den sozialen Medien
Twitter @ZVKI_de
Instagram @zvki.de

oder registrieren Sie sich auf zvki.de für unseren Newsletter.

Anzeige

Datenschutzmanagement
einfach und sicher per Software abdecken.

Mithilfe von Proliance 360 können Sie Datenschutz digital abdecken – sowohl intern, wie auch extern.

Exklusiv für BvD Mitglieder:
Sichern Sie sich ein Digitalisierungsbudget von **bis zu 300€**.

Exklusiv für BvD Mitglieder

Mithilfe des QR-Codes können Sie schnell und einfach ihren Termin vereinbaren. Selbstverständlich unverbindlich und kostenlos.

DATENSCHUTZ EXPERTE.DE
ein Service der Proliance GmbH

WAS KOMMT AUS BRÜSSEL UND WASHINGTON AUF DIE DSB ZU?

Die BvD-Herbstkonferenz diskutiert Leitfragen eines künftigen europäischen und transatlantischen Datenschutzes.

DIE BVD-HERBST-KONFERENZ

Die Konferenz-Partner: Die BvD-Herbstkonferenz und der Behördentag sind eine Initiative des BvD mit dem Bayerische Landesamt für Datenschutzaufsicht, dem Landesbeauftragten für Datenschutz Bayern sowie dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI). Die Konferenz findet alternierend in Bayern und Baden-Württemberg statt. Nach der Tagung in München 2021 reisten in diesem Jahr rund 350 Teilnehmende zu Herbstkonferenz und Behördentag nach Stuttgart.

Zur nächsten Herbstkonferenz laden der BvD und die Aufsichtsbehörden aus Bayern und Baden-Württemberg wieder nach München. Die Tagung findet vom 18. bis 20. Oktober 2023 statt.

Traditionell widmen sich die BvD-Herbstkonferenz und der anschließende Behördentag aktuellen Entwicklungen beim Datenschutz. Auf der sechsten Ausgabe der Tagung vom 26. bis 28. Oktober in Stuttgart standen die digitalen Acts der EU und der neue Anlauf für ein Privacy Shield zwischen den USA und der EU im Mittelpunkt von Vorträgen und Debatten. Der Präsident des Bayerischen Landesamts für Datenschutz (LfDA), Michael Will, appellierte zum Auftakt an die rund 250 betrieblichen und etwa 100 behördlichen Datenschutzbeauftragten in Stuttgart sich rechtzeitig mit den Gesetzesvorhaben Data Act, Digital Services Act, Digital Markets Act und Artificial Intelligence Act auseinanderzusetzen. Denn durch sie könnten durchaus weitere Aufgaben auf die Landesdatenschutzbeauftragten, aber auch auf betriebliche wie behördliche Datenschutzbeauftragte zukommen. „Schauen Sie nach Leitlinien des Europäischen Datenschutzausschusses, nicht nach Kurzpapieren der deutschen Datenschutzkonferenz“, empfahl Will den Teilnehmenden.

Die BvD-News dokumentiert nachfolgend Key-Notes der Tagung:

Wie hat die EU den Datenschutz verändert?

Renate Nikolay, Kabinettschefin der Viizepräsidentin der EU-Kommission und Kommissarin für Werte und Digitales, Véra Jourová

Mit dem Data Act, dem Digital Markets Act, dem Data Governance Act und dem AI Act will die EU die großen Daten-Unternehmen wie

Renate Nikolay

Google oder Meta auf das europäische Datenschutzverständnis verpflichten. Dahinter steht die Erkenntnis, dass die digitale Transformation nur mit einem funktionierenden Datenschutz gelingen kann. Ziel ist es mit der Gesetzgebung den Wilden Westen der Digitalisierung zu beenden und Ordnung in die Nutzung von Daten innerhalb Europas zu bringen. Auch wenn die EU-Kommission bereits seit langem um einen Weg ringt, Betroffene in der EU besser vor Datenmissbrauch zu schützen, wurden der Data Act und der Data Governance Act sehr schnell entwickelt. Deshalb seien im Gesetzgebungsverfahren kritische Stimmen sehr wichtig. Die EU-Kommission versucht viel zu erreichen und einen konträren Ansatz etwa zu den datengetriebenen Unternehmen im amerikanischen Silicon Valley zu etablieren. Jetzt geht es aber erst einmal darum diese Rechtsakte umzusetzen und zu sehen, dass sie funktionieren.

Die EU hat ein großes Versprechen gegeben: Die großen Plattformen zu kontrolllieren. Damit hat sie sich einmal mehr neben der DSGVO beim Datenschutz zum Referenzpunkt für die Welt gemacht. Gerade die USA beneiden uns um unser Datenschutzregime, weil sie erkennen, dass in ihrem Land die Zersplitterung beim Datenschutz kaum mehr einzufangen ist. Datenschutz made in Europe, der den Menschen in den Mittelpunkt stellt, wird zu einem Momentum zwischen autokratischen und demokratischen Staaten. Deshalb müssen wir die strategischen Allianzen mit den Staaten verfestigen, die so denken wie wir. Und dazu gehören auch die USA. Ich bin zuversichtlich, dass wir mit den USA ein Abkommen erarbeiten werden, dass vor einer weiteren Klage von Max Schremms vor dem Europäischen Gerichtshof Bestand haben wird.

Ganz allgemein zeigt die DSGVO in ihrem fünften Jahr, dass sie durchaus Zähne entwickelt hat: Mehr und mehr treffen die Aufsichtsbehörden in den Mitgliedsstaaten große Bußgeld-Entscheidungen, die sich bis jetzt auf rund 1,5 Milliarden Euro summiert haben. Zudem wird die Kooperation der Aufsichtsbehörden bei grenzüberschreitenden Streitfällen geschmeidiger. Gleichwohl wollen wir die Zusammenarbeit der EU-Staaten untereinander und mit dem Europäischen Ausschuss für Datenschutz stärken. Ebenso müssen wir die Aufklärungsarbeit für kleine und mittlere Unternehmen fortsetzen und die proaktive Dialogbereitschaft der Datenschutzaufsichtsbehörden mit den Bürgern und Unternehmen unterstützen.

Dr. Jan Wacke

Welche Auswirkungen hat die Pandemie auf den Datenschutz?

Dr. Jan Wacke, Leitender Beamter des LfDI Baden-Württemberg

In der Pandemie wurden verschiedene Grundrechte eingeschränkt, darunter die Versammlungsfreiheit, die Gewerbe- und Berufsfreiheit und die Bewegungsfreiheit. Aber auch in das Datenschutz-Grundrecht wurde vielfach eingegriffen; man denke an die Kontaktdatenerfassung in Cafés und Restaurants, die Offenlegung von Gesundheitsdaten und anderen sensiblen Informationen in vielen alltäglichen Situationen oder beispielsweise die Verarbeitung von Gesundheitsdaten durch den Arbeitgeber. Im Großen und Ganzen waren diese auf die Pandemiebekämpfung zweckgerichteten Maßnahmen mit der DSGVO vereinbar. Diese hat sich selbst in der Krisensituation unter anderem wegen ihrer Öffnungsklauseln als flexibel genug erwiesen.

Zwar waren einzelne Aspekte dieser Regelungen zur Pandemiebekämpfung problematisch. Oft haben die Gesetz- und Verordnungsgeber die Beratungspflicht aus Artikel 36 Absatz 4 DSGVO nicht eingehalten. Datenschutzrechtliche Mängel einzelner Normen (z. B. die Unterscheidung von gesetzlichen Verarbeitungen/Verarbeitung kraft Einwilligung, die Gewährleistung angemessener und spezifischer Maßnahmen im Sinne von Artikel 9 Absatz 2 Buchstabe i DSGVO etwa durch Anordnung einer gesetzlichen Geheimhaltungspflicht für Testzentren) hätten bei Durchführung des Konsultationsverfahrens eventuell vermieden werden können. Das hätte – durch Verminderung der Anzahl der Regelungsänderungen – auch zu einer besseren Akzeptanz der Normen beitragen können. Ein Grundproblem der Normgeber in der Krise war dabei aber sicher die Eilbedürftigkeit des regularischen Handelns.

Neben regulatorischen Eingriffen gab es im Regelungsvollzug zahlreiche praktische Defizite bei der Umsetzung datenschutzrechtlicher Anforderungen. Besonders hervorzuheben sind etwa die Mängel des technischen und organisatorischen Datenschutzes bei der Kontaktdatenverarbeitung oder bei Testzentren.

Auf anderer Ebene förderte die Pandemie tiefgreifende gesellschaftliche Entwicklungen: Sie forcierte das bargeldlose Bezahlen, etablierte die digitale Kommunikation beruflich wie

privat als neuen Standard und gab einen enormen Schub für die Digitalisierung in Schulen, an Hochschulen und im Gesundheitsbereich. Leider hat die Digitalkompetenz nicht Schritt gehalten und oft einem unkritischen Digitalisierungsglauben den Weg bereitet.

Als mittelbare Folge der Pandemie rückte auch der Umgang mit Forschungsdaten im Gesundheitsbereich stärker in den Fokus (auch wenn die damit verbundene nationale und europäische Gesetzgebung wohl kaum ausschließlich als Mittel zur Pandemiebewältigung begriffen werden kann). Gerade bei der Forschung mit Gesundheitsdaten muss Datenschutz als Bedingung für die Akzeptanz der Datenverarbeitung begriffen werden.

Es geht beim Datenschutz in der Forschung also nicht nur um das individuelle Interesse einzelner Betroffener, das gegen das Interesse der Gemeinschaft an Fortschritt durch Forschung abzuwägen wäre. Sondern an der Wahrung des Datenschutzes besteht mit Blick auf die Akzeptanz (etwa auch des die Daten „produzierenden" Gesundheitssystems) zugleich ein öffentliches Interesse. Die Wahrung des Datenschutzes liegt damit mit anderen Worten – auch und gerade bei der Forschung mit Gesundheitsdaten – letztlich im Interesse des Verantwortlichen.

Während der Pandemie wurde zuweilen „der Datenschutz" als „Supergrundrecht" gebrandmarkt, das solche Entwicklungen und die Pandemiebekämpfung hindere. Woher rührte diese (unzutreffende) Wahrnehmung? Anders als andere Grundrechte hat die informationelle Selbstbestimmung mit Blick auf die für den einzelnen schwer durchschaubaren Gefährdungen und die geringen Abwehrmöglichkeiten des einzelnen spezielle „Wächter" an die Seite gestellt bekommenen in Form von Datenschutzaufsicht und Datenschutzbeauftragten. In der Pandemie wurde vielfach rechtliches Neuland betreten, zu dem es noch keine Rechtsprechung gab. Mit Blick auf die Länge gerichtlicher Verfahren gab es kaum Orientierung durch die dritte Gewalt. Dadurch rückten die „Datenschutzwächter" stärker in den Fokus. Die Pandemie hat auf der anderen Seite beispielhaft gezeigt, dass Datenschutz und Digitalisierung sehr gut zusammenpassen, ja einander fördern können (etwa durch die Corona-Warn-App und die Luca-App).

Nach der Pandemie kommt uns Aufsichtsbehörden nun die Aufgabe zu zunächst zu schauen, wo und wann überhaupt noch eine „Pandemie" gegeben ist, zu deren Bewältigung Eingriffe in den Datenschutz (noch) notwendig wären. Nicht mehr notwendige Verarbeitungen sind einzustellen, nicht mehr notwendige Daten zu löschen. In Baden-Württemberg beispielsweise sind wir mit einer Reihe von Start-Ups im Gesundheitsbereich im Gespräch, wie Datennutzung und Datenschutz zusammengehen können.

Alexander Filip

Wie geht es mit dem Datentransfer in die USA weiter?

Alexander Filip, Geschäfts- und Bereichsleiter für internationalen Datentransfer beim Bayerischen Landesamt für Datenschutzaufsicht

Sprechen wir über den Datentransfer in Drittstaaten stellt sich schnell heraus, dass allein diese Formulierung viele Fragen aufwirft. In der Auslegung des Europäischen Datenschutz-Ausschusses EDSA im Leitlinienpapier Nr. 5/2021 vom 18.11.2021 ist festgehalten, was überhaupt als Datentransfer in ein Drittland zu verstehen ist. Aktuell arbeitet die EDSA an einer zweiten Version. Ob diese bis Ende des Jahres vorliegen wird, ist noch offen.

Nach der aktuellen ersten Version spricht der EDSA von Datentransfer in ein Drittland, wenn ein Verantwortlicher oder ein Auftragsverarbeiter an einen anderen Verantwortlichen oder Auftragsverarbeiter in einem Drittland personenbezogene Daten übermittelt. Die Daten fließen also von einem Verantwortlichen oder Auftragsverarbeiter zu einem anderen. Die Endfassung des Papiers bleibt abzuwarten, es könnte noch zu einigen Präzisierungen kommen, das ist derzeit aber noch in der Diskussion. Nicht immer einfach ist es in der Praxis zu bestimmen, welche datenschutzrechtliche Rolle ein Datenempfänger in einem Drittland im konkreten Fall hat. Davon hängt aber die Antwort auf die Frage ab, ob eine Übermittlung in ein Drittland gemäß der oben dargestellten Interpretation des EDSA vorliegt: Die Datenoffenlegung ist nur dann eine Übermittlung in ein Drittland, wenn der Empfänger im Drittland als vom Übermittler gesonderter, zu unterscheidender Auftragsverarbeiter oder eigenständiger Verantwortlicher einzustufen ist. Es gibt eine Reihe von Szenarien, über die man hier trefflich diskutieren kann. Die Aufsichtsbehörden prüfen, ob weitere solche Szenarien in der Endfassung des oben genannten Papiers beispielhaft genannt und rechtlich entsprechend eingeordnet werden. Wenn etwa ein Mitarbeiter auf Geschäftsreise sich per Fernzugriff in das

Intranet der Heimatfirma einloggt und dabei Zugriff auf personenbezogene Daten nimmt, wertet der EDSA dies nicht als Übermittlung in ein Drittland, weil der Mitarbeiter eben kein separater Verantwortlicher oder Auftragsverarbeiter ist. Aber könnten nicht die von dem Mitarbeiter genutzte Infrastruktur im Drittland oder die dort bestehenden Zugriffsmöglichkeiten für dortige Behörden die Nutzung der Daten unsicher machen? Diese Frage ist valide und zeigt, dass den spezifischen Risiken, die sich aus der Drittlandsberührung ergeben, auch dann Rechnung getragen werden muss, wenn das Szenario rechtlich nicht als „Übermittlung in ein Drittland" gewertet wird - in dem Szenario des reisenden Mitarbeiters beispielsweise im Rahmen von Maßnahmen nach Artikel 32 DSGVO.

Ein weiterer möglicher Streitfall: Ein Unternehmen aus Europa unterhält in den USA einen eigenen Server. Auch hier sieht der erste EDSA-Entwurf keinen Datentransfer in ein Drittland. Aber was ist mit den Risiken, die sich aus dem Betrieb des Servers im Drittland ergeben? Auch hier gelten oben genannte Überlegungen entsprechend.

Ebenfalls sieht der EDSA keinen Datentransfer, wenn ein Unternehmen in Europa Daten an eine Niederlassung beispielsweise in Singapur übermittelt – außer, wenn die Niederlassung im konkreten Fall als separater Auftragsverarbeiter (oder Verantwortlicher) einzustufen ist.

Zu Google Analytics teilen wir die rechtliche Bewertung der Aufsichtsbehörden in Österreich, Frankreich und Italien, die dazu bereits Anordnungen erlassen haben – wonach die Weitergabe von personenbezogenen Daten im Rahmen des Einsatzes von Google Analytics (jedenfalls in der Cookie-basierten Variante) gegen Kapitel V DSGVO verstößt, weil die von Google angebotenen „zusätzlichen Maßnahmen" aus Sicht der genannten Behörden und auch des BayLDA nicht ausreichen, um ein mit dem EU-Datenschutzniveau gleichwertiges Schutzniveau zu gewährleisten. Denkbar sind Google-Analytics-Varianten, bei denen ein sogenanntes Server Side Tracking gemacht wird, also wenn das Tool ohne Einsatz eines Cookies und ohne darin enthaltene eindeutigen IDs verwendet wird. Allerdings kann der Einsatz auch in dieser Variante nur bei Erfüllung weiterer Voraussetzungen zulässig sein – nämlich nur, wenn auch unabhängig vom Fehlen von eindeutigen IDs darüber hinaus an Google keine Daten übermittelt werden, die eine Identifizierung des Nutzers ermöglichen. Die französische Datenschutzbehörde hat auf ihrer Website hierfür eine Reihe von Anforderungen genannt, die vom BayLDA geteilt werden. Ob das Tool für das nutzende Unternehmen unter diesen Voraussetzungen überhaupt interessant ist, ist dann eine andere Frage.

Eine weitere häufig gestellte Frage ist die nach der Datenschutzkonformität von Microsoft 365. Andes als die Aufsichtsbehörde in Baden-Württemberg hat das BayLDA keine umfassende datenschutzrechtlichen Bewertung zum Einsatz dieser Software etwa an Schulen unternommen. Die Aufsichtsbehörde Baden-Württemberg sah unter anderem Unklarheiten dahingehend, welche Daten insgesamt Microsoft für welche Zwecke verarbeitet. Nach den dem BayLDA bislang vorliegenden Erkenntnissen jedenfalls sehen wir derzeit beim Einsatz von MS365 keinen Sachverhalt, der es gebieten würde aufsichtliche Maßnahmen bezogen auf den Einsatz von Microsoft 365 bei den der Aufsicht des BayLDA unterliegenden Stellen zu ergreifen.

Die von US-Präsident Joe Biden vorgestellte Executive Order, die Teil des Nachfolgeregimes zum EU-US Privacy Shield werden soll, erscheint als ein nicht unbedeutender Fortschritt gegenüber den früheren Standards unter dem alten Privacy Shield. Insbesondere für das beim US-Justizministerium anzusiedelnde Datenschutzgericht, bei dem betroffene Personen aus der EU, deren Daten in die USA übermittelt wurden, Rechtsschutz suchen können, scheinen offenbar bei überschlägiger erster Durchsicht doch einige Fortschritte im Hinblick auf die Unabhängigkeit und die Handlungskompetenzen dieses Gremiums erzielt worden zu sein. Das ist jedenfalls eine Verbesserung gegenüber der Ombudsperson, die im EU-US-Privacy Shield verankert war und die der EuGH im Schrems-II-Urteil als unzureichend einstufte.

Allerdings müssen die in der Executive Order angelegten Änderungen auf Seiten der USA erst noch umgesetzt werden. Hierzu gehören neben der Einrichtung des oben genannten Datenschutzgerichts eine Reihe von Änderungen in den internen Verfahrensregelungen und Policies verschiedener US-amerikanischer Nachrichtendienste; die Executive Order sieht insoweit vor, dass Änderungen erfolgen sollen, die den vom Europäischen Gerichtshof angemahnten Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit von Datenzugriffen Rechnung tragen sollen. Bis jetzt sind diese Änderungen noch nicht abgeschlossen. Erst wenn die US-Seite dies gegenüber der Europäischen Kommission bestätigt, wird die Kommission den als Nachfolgeregelung zum Privacy Shield vorgesehenen Beschluss erlassen können. Solange die Änderungen noch nicht umgesetzt sind, kann seitens europäischer Unternehmen, die Daten in die USA übermitteln möchten, auch noch nicht davon ausgegangen werden, dass die vom Europäischen Gerichtshof identifizierten Probleme bei der Situation in den USA abgestellt sind.

Über die Autorin

Christina Denz

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

Foto: Eckhard Henkel / Wikimedia Commons / CC BY-SA 3.0 DE

VOM BONNER TULPENFELD ZUM HOCHSCHUL-CAMPUS IN ULM

Wie sich der BvD gründete

Prof. Dr. Gerhard Kongehl, Dr. Bernd Beier

Im Jahre 1987 las Bernd Beier einen Artikel von Gerhard Kongehl in der Zeitschrift Datenschutz und Datensicherheit (DuD)[1] und einen Artikel über Gerhard Kongehl im SPIEGEL[2]. Daraufhin meldete sich Bernd Beier telefonisch bei Gerhard Kongehl in Ulm.

Bernd Beier war damals unter anderem Datenschutzbeauftragter der Unicardan AG, zuvor Leiter der Datenschutzabteilung des Klinikums der Universität Frankfurt/Main und Dozent am College of Engineering der University of Maryland/USA. Gerhard Kongehl war damals an der Universität Ulm sowohl in der Hirnforschung als auch im Datenschutz aktiv. Als Hirnforscher war er auch Dozent für Wahrnehmungspsychologie an der Hochschule für Gestaltung. Als Datenschützer übte Kongehl die Funktion des Datenschutzbeauftragten der Universität und des Klinikums der Universität aus und war überdies auch Dozent für Datenschutz an der Ulmer Fachhochschule.

Die beiden tauschten sich nun über ihre jeweiligen Erfahrungen in ihrer Rolle als Datenschutzbeauftragte aus und sie beklagten sich beide in diesem Zusammenhang auch ganz allgemein über die mangelnde Unterstützung der betrieblichen und behördlichen Datenschutzbeauftragten durch die GDD, die damals noch Gesellschaft für Datenschutz und Datensicherung hieß und zu jener Zeit die einzige Institution zur Vertretung der Belange des Datenschutzes war. Man war sich in dem Telefonat einig, dass die GDD eher die Interessen von Unternehmen gegenüber dem Datenschutz vertrete als die Vertretung des Datenschutzes im Interesse der Gesellschaft. Bernd Beiers Fazit dieses Telefonats war, dass man eine eigene Interessenvertretung der betrieblichen und behördlichen Datenschutzbeauftragten gründen müsste, Gerhard Kongehl war noch skeptisch. Er fragte sich, ob man in der Lage sein würde die hierzu erforderliche Energie aufzubringen, da dies ja eine Gründung gegen die damals schon recht einflussreiche GDD sein müsste.

Erstes Treffen im Bonner Tulpenfeld

Man plante aber den Vorschlag von Bernd Beier weiter bei einem Treffen zu diskutieren. Diese Möglichkeit bot sich sogar schon recht kurzfristig, weil Gerhard Kongehl mit seinen Studierenden der Datenschutzausbildung an der Fachhochschule Ulm eine Exkursion zum Deutschen Bundestag (damals noch in Bonn) plante, wobei unter anderem auch Diskussionen mit den politischen Parteien im Bonner Tulpenfeld (damals ein Zentrum der Bonner Politik) geplant waren. Hier trafen sich in der Abgeordneten-Kantine am Tulpenfeld dann auch zu ersten Mal Bernd Beier und Gerhard Kongehl persönlich. Und man war sich schnell einig, dass man durchaus in der Lage sei eine eigene Interessenvertretung der Datenschützer zu gründen, denn mit den Datenschutz-Dozenten der Fachhochschule Ulm und ihren Studierenden verfüge man ja durchaus über das erforderliche Gründungspotential. Seit dem Treffen am Tulpenfeld in Bonn blieben Bernd Beier und Gerhard Kongehl ständig in Kontakt, um ihre Gründungsidee weiter zu verfolgen. Das erste zu lösende Problem war die Namensgebung. „Gesellschaft der Datenschutzbeauftragten" wäre angemessen gewesen, hätte aber womöglich Konflikte mit der GDD und eventuell auch mit der Gesellschaft für Informatik (GI) bedeutet. Weil man sich aber durchaus als Alternative zur GDD empfand, erschien es ihnen zu bieder sich lediglich als „Verein" zu bezeichnen - obwohl man sich als gemeinnützigen Verein gründen wollte. So kam man schließlich auf den Begriff „Verband". Kongehl war zunächst für „Bundesverband der betrieblichen und behördlichen Datenschutzbeauftragten", Beier für Berufsverband der betrieblichen und behördlichen Daten-

schutzbeauftragten. Obwohl „Bundesverband" irgendwie bedeutender klingt als „Berufsverband" entschied man sich doch für letzteres, weil sich herausstellte, dass man allein schon mit dem Begriff „Verband" bei der Eintragung beim Registergericht Ulm Schwierigkeiten bekommen würde. Als Verband, so teilte man ihnen mit, verstehe man immer eine Dachorganisation einer Mindestanzahl von Vereinen. „Berufsverband" könnte vielleicht leichter durchzusetzen sein als Bundesverband. „Berufsverband" passte schließlich auch, denn man wollte ja (neben der Förderung und Weiterentwicklung der Idee „Datenschutz") vor allem auch eine berufsständische Vertretung der Datenschützer sein.

Um mit dem Begriff „Verband" vom Registergericht Ulm akzeptiert zu werden, gründete man deshalb zunächst fünf lokale Datenschutzvereine, die als Regionalgruppen funktionierten: In Ulm (Baden-Württemberg), Neu-Ulm (Bayern), Stuttgart, Frankfurt/Main und in München. Außerdem verwendete man in der Satzung den Begriff „Verband" weitgehend nur in der Bezeichnung nach außen. Im Text der Satzung selbst wurde aber fast immer der Begriff „Verein" verwendet. Oberflächlich betrachtet, erschien das widersprüchlich. Aus strategischen Gründen glaubte man aber so verfahren zu sollen.

1989: Gründung des BvD e.V.

Mit Gerhard Kongehl als Vorsitzendem, Bernd Beier als stellvertretendem Vorsitzenden, Armin Herb als Justiziar und einigen weiteren Dozenten und Studierenden der Ausbildung von Datenschutzbeauftragten der FH Ulm gründete man im Jahre 1989 dann den „Berufsverband der betrieblichen und behördlichen Datenschutzbeauftragten Deutschlands (BvD) e.V.". Übrigens hatte man damals auch mit der Abkürzung BvD Probleme, weil es unter dieser Bezeichnung in den USA eine bekannte Firma für Herren-Unterwäsche gab und gibt (www.bvd.com). Man beschloss aber die Abkürzung trotzdem beizubehalten, als Webadresse aber sicherheitshalber auf www.bvdnet.de auszuweichen.

Wer glaubte, mit der Bezeichnung „Berufsverband der betrieblichen und behördlichen Datenschutzbeauftragten Deutschlands (BvD) e.V." wären alle Klippen umsegelt worden, musste sich leider eines Besseren belehren lassen. Das Registergericht Ulm lehnte jetzt auch diese Bezeichnung ab, da nach Auffassung dieses Gerichts betriebliche und behördliche Datenschutzbeauftragten keinen Beruf ausüben würden. Natürlich empfand man das als eine unglaubliche Provokation und hatte deshalb sofort gegen diese Entscheidung geklagt und Herrn Professor Spiros Simitis, Doktorvater von Bernd Beier, der bei Simitis zum Thema „Datenschutz in der Medizin" an der Juristischen Fakultät der Goethe-Universität zu Frankfurt promoviert hatte, zur Unterstützung um ein entsprechendes Gutachten gebeten. Herr Simitis kam dankenswerter Weise dieser Bitte sehr gerne nach. Sein Gutachten überzeugte das jetzt zuständige Landgericht Ulm, indem es seine Argumente fast vollständig übernahm. So hatte das Gericht Ulm in seinem Beschluss festgestellt (Az.: 5T 153/90-01 LG Ulm), dass betriebliche und behördliche Datenschutzbeauftragte doch einen Beruf ausüben würden, weil sie mit ihrer Tätigkeit einen auf Dauer berechneten und nicht vorübergehenden Beitrag zur gesellschaftlichen Gesamtleistung erbringen würden. Auch wenn sie ihre Aufgabe als Datenschutzbeauftragte nur neben ihrem eigentlichen Hauptberuf ausüben würden, sei diese Tätigkeit aus verfassungsrechtlicher Sicht als Beruf anzusehen. Weiter führte das Gericht aus, dass auch wenn das damals zuständige Bundesdatenschutzgesetz die Tätigkeit als Datenschutzbeauftrage(r) nicht von einem bestimmten Ausbildungsgang abhängig mache, dennoch zahlreiche Einzelregelungen des Gesetzes für das Vorliegen eines relativ konkreten Berufsbildes spräche. Das Gesetz verlange von den Datenschutzbeauftragten die erforderliche Fachkunde und Zuverlässigkeit. Gerade an die Fachkunde würden hohe Anforderungen gestellt. Im Folgenden machte das Gericht dann auch konkrete Ausführungen wie eine Ausbildung zur Erlangung dieser Fachkunde auszusehen habe[3].

Damit war endlich der Weg frei für die Gründung des „Berufsverbandes der betrieblichen und behördlichen Datenschutzbeauftragten Deutschlands (BvD) e.V.". Im Frühjahr 1988 im Bonner Tulpenfeld gezeugt, kam er im Herbst 1990 in der Aula des Campus der Technischen Hochschule in Ulm zur Welt. Ursprünglich führte man zur Abgrenzung vom Bundesbeauftragten und den Landesbeauftragten für den Datenschutz noch die Bezeichnung „betriebliche und behördliche…" im Namen. Später gab man diesen Zusatz auf und seitdem nennt sich der BvD „Berufsverband der Datenschutzbeauftragten (BvD) e.V.". Und das bis heute.

Über die Autoren:

Prof. Dr. rer. nat. Gerhard Kongehl
war BvD-Gründungsmitglied, bis 2004 Bundesvorsitzender und ist heute Ehrenmitglied des BvD. Der promovierte Physiker begann seine Datenschutzlaufbahn 1978 als erster Datenschutzbeauftragter Baden-Württembergs, 1983 erhielt er durch die Ulmer Hochschulen den ersten Lehrauftrag im Fach Datenschutz in Baden-Württemberg. Seit 1993 ist Kongehl Professor für Datenschutz, Datensicherheit und Technikfolgenabschätzung der Fachhochschule Ulm. Er ist zudem Gesellschafter, Geschäftsführer und wissenschaftlicher Leiter der Ulmer Akademie für Datenschutz und IT-Sicherheit, udis gGmbH. Er ist Herausgeber einer Vielzahl von Fachpublikationen und Träger des Bundesverdienstkreuz für seine Verdienste um den Datenschutz.

Dr. iur. Bernd Beier
war Mitbegründer des BvD. Neben praktischer beruflicher Tätigkeit und Hochschul-Lehre zahlreiche wissenschaftliche Publikationen, insbesondere zu Datenschutzrecht und Recht der Informationstechnologie.

[1] Gerhard Kongehl: Müsste man den Computer nicht abschalten? Ethische Probleme der Computernutzung in der Krankenversorgung. Datenschutz und Datensicherheit (DuD); S.163-175. Vieweg Verlag Wiesbaden (1987)

[2] Der Spiegel: Null Kenntnis – Erstmals können sich Studenten zum Datenschützer ausbilden lassen. Der Spiegel 46; S. 93 (1987).

[3] https://www.udis.de/doc/DuD_2007-05_Ausbildung_Datenschutzbeauftragter_Das_Ulmer_Modell.pdf

MITGLIEDERVERSAMMLUNG BESCHLIESST EINSTIMMIG NEUE SATZUNG

In über 30 Jahren BvD hat sich viel geändert – an der Arbeit und dem Berufsbild von Datenschutzbeauftragten, aber auch daran, wie Verbände zeitgemäß arbeiten. Zudem ist die Zahl der Mitglieder insbesondere in den letzten Jahren massiv gestiegen. Daher war die Zeit für eine umfassende Modernisierung der BvD-Satzung gekommen. Den Antrag auf Neufassung der Satzung stellte der Vorstand zur ordentlichen Mitgliederversammlung im Mai 2022. Da hier das Quorum nicht erreicht wurde, wurde anschließend zu einer außerordentlichen Mitgliederversammlung eingeladen, die unabhängig von der Zahl der Teilnehmenden beschlussfähig war und die die Neufassung am 25. Oktober 2022 in Stuttgart mit 44 Ja-Stimmen einstimmig beschlossen hat.

Wir sagen DANKE!

An der Neufassung haben neben den Vorstandsmitgliedern viele weitere Menschen mitgewirkt, denen an dieser Stelle zu danken ist:

- Der Ausschuss Satzung, an dem sich über die Jahre Svenja Arndt, Stephan Eschenbacher, Karsten Füllhaase, Klaus Schrenk, Claudia Seilert, Peter Stahlberg und Barbara Stöferle beteiligt haben
- Der Sprecherkreis des BvD
- Vereinsrechtler RA Alexander Winkel

Darüber hinaus sind Hinweise von mehreren Mitgliedern bei der Aussprache zur neuen Satzung auf der ordentlichen Mitgliederversammlung sowie bei der im April 2022 durchgeführten Online-Informationsveranstaltung eingeflossen.

Das Wichtigste vorab: Es gibt *keine* materielle Änderung des Vereinszwecks. Die Änderungen an §2, der den Zweck enthält, konkretisieren den Zweck, ohne dass Zwecke gestrichen oder jemand aus dem Vereinszweck ausgeschlossen würde. Viele Änderungen dienen lediglich dazu Begrifflichkeiten zu vereinheitlichen und veraltete Begrifflichkeiten an die heutige, durch Digitalisierung geprägte Realität anzupassen. Zudem tragen einige Ergänzungen bei den Verbandsaufgaben wichtigen Kernprojekten des BvD Rechnung, beispielsweise im Bereich der Zertifizierung oder der Vernetzung des BvD im europäischen Dachverband EFDPO.

Längst überfällig waren Änderungen, die eine Kommunikation mit allen aktuell gängigen Kommunikationsmitteln zulassen. Das gilt sowohl für Kommunikation in Textform (zum Beispiel den Einladungsversand zur Mitgliederversammlung) als auch für die Art, wie heutzutage Treffen, Versammlungen sowie Beschlüsse und Abstimmungen gehandhabt werden. All das ist nicht nur komfortabler für alle Beteiligten, es schont auch die Umwelt und Verbandsressourcen.

Wenn es um Mehrheiten und Quoren in der Satzung geht, so wurde diese zur Gründung des Verbands bewusst hoch angesetzt. So sollte verhindert werden, dass eine kleine Gruppe schnell massiven Einfluss gewinnen und den Verband an sich reißen kann. Was seinerzeit eine wichtige Schutzfunktion erfüllte, schränkt bei der heutigen Größe des Verbands die Handlungsfähigkeit des BvD erheblich ein. Entsprechende Änderungen in der Satzung schaffen daher nun einen sinnvollen, der Verbandsgröße angemessenen Ausgleich zwischen Schutz vor Fremdübernahme und Erhalt der Handlungsfähigkeit.

Ist die alte Satzung an manchen Stellen bewusst restriktiv, so vereinte sie sehr hohe Entscheidungsgewalt in der Person des Vorstandsvorsitzenden, der ein Alleinvertretungsrecht hat. Dies wurde nun dahingehend geändert, dass immer zwei Personen *gemeinsam* den BvD gerichtlich und außergerichtlich vertreten. Außerdem wird die Amtszeit des Vorstands von zwei auf drei Jahre geändert.

Die Neufassung der Satzung wurde nach der Mitgliederversammlung beim Amtsgericht Charlottenburg zur Eintragung in das Vereinsregister angemeldet. Sie tritt unmittelbar nach Eintragung in Kraft und wird auf der BvD-Website veröffentlicht. Bis dahin finden Mitglieder die Neufassung bei den Unterlagen zur außerordentlichen Mitgliederversammlung im Mitgliederbereich der BvD-Website. kfh

WEITERBILDUNG FÜR DIE LEBENSWELT VON KINDERN UND JUGENDLICHEN

Neue Perspektiven auf dem Dozent:innentag von „Datenschutz geht zur Schule“

Der Weg nach Kiel war für die meisten der Ehrenamtlichen von „Datenschutz geht zur Schule“ (DSgzS) ein weiter – aber auch ein lohnender. Denn wer im September zum Dozent:innentreffen 2022 der Initiative fuhr, durfte sich über eine Eintrittskarte zur Sommerakademie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) freuen. ULD-Chefin **Marit Hansen** war dementsprechend eine der Vortragenden auf dem Dozent:innentag, der an die Sommerakademie anschloss.

Der Fokus des Treffens lag auf der Lebenswelt der Kinder und Jugendlichen, vor denen die Dozent:innen der Initiative ihre Vorträge halten. Den Auftakt lieferte die Juristin **Lisa Pommerening** mit dem Thema Profiling bei Kindern, am Beispiel der Video-Plattform Tiktok. Da Kinder nicht abschätzen könnten und auch nicht abschätzen müssten, was dabei passiere, hält sie die Video-Plattform für Minderjährige schlicht für ungeeignet.

Franziska Drauz setzte bei den Lehrkräften an. Ihr gemeinnütziges Unternehmen Zukunft Digitale Bildung schult Lehrer:innen für das digitale Arbeiten und den digitalen Alltag an Schulen. Ihr Fazit: „Es besteht eine große Diskrepanz zwischen dem Bildungsangebot am Markt und dem, was in Schulen aktiv eingesetzt wird.“ Hier müsse man Brücken bauen.

Michela Luliano vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI) will mit der Initiative „Informationsfreiheit geht zur Schule“ ein aktives demokratische Leben unter den Jugendlichen stärken.

Professor **Steffen Kroschwald** von der Hochschule Pforzheim präsentierte, wie er seine Studierenden anhand eines fiktiven App-Projekts für Datenschutzfragen begeistert. Sein Ansatz: „Schutz, Selbstbestimmung und damit aktive Teilhabe an der digitalen Gesellschaft“

Tatjana Halm von der Verbraucherzentrale Bayern stellte die vielen interaktiven und jugendgerechten Informations- und Sensibilisierungsangebote der Verbraucherschützer vor.

Marit Hansen warb dafür, bei allen Fragestellungen immer die Auswirkungen auf die Menschen und damit die Auswirkungen auf die Gesellschaft im Blick zu behalten.

Foto: Christina Denz

Sicherheitsexperte **Gerhard Klostermeier** vom Pentest-Anbieter SySS demonstrierte, wie sich Zugangskarten, wie sie für Hoteltüren und Schließsysteme an Hochschulen üblich sind, auf einfachste Weise kopieren und missbrauchen lassen.

Zum Abschluss verriet Rechtsanwalt **Chan-jo Jun**, wie er seine Vorträge für Jugendliche auf der Höhe der Zeit hält: Junge Mitarbeiter:innen müssten fortlaufend seine Prezi-Präsentation aktualisieren. Sein Joker: Er weist Schülerinnen und Schüler auf ihre zivilrechtliche Haftung hin, die bereits vor der Strafmündigkeit ab 14 Jahren einsetzt.

Unterstützt wurde der Dozent:innentag von der DATEV Stiftung Zukunft und dem WEKA Verlag. *dhb*

KUNST FÜR DEN LFDI

Foto: Christina Denz

Der Künstler Florian Mehnert hat eigens für die Geschäftsstelle des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) in Stuttgart ein Kunstwerk geschaffen. Die begehbare Lichtkunstinstallation „data to light" erstreckt sich über zwei Etagen und will „die unsichtbare Arbeit des Datenschutzes und der Informationsfreiheit sichtbar machen", wie Mehnert erläutert.

Von vielen Arbeitsräumen führt jeweils ein farbiger LED-Streifen an den Wänden und Fluren entlang hin zum Mittelpunkt der jeweiligen Etage, wo sich die Streifen zu einer bunten Lichtsäule vereinen, die die dritte und vierte Etage visuell verbindet. Damit solle laut Mehnert veranschaulicht werden, „wie einzelne Mitarbeitende als individuelles Element der Datenschutzbehörde mit ihrer täglichen Arbeit unsere Daten und Freiheit schützen und dabei ihre Energie bündeln und konzentrieren."

Clarissa Henning, die persönliche Referentin des erkrankten LfDI Dr. Stefan Brink führte Interessierte zum Auftakt der BvD-Herbstkonferenz in Stuttgart durch die Installation.

Mehnert beschäftigt sich seit Langem künstlerisch mit den Themen Datenströme, Datenschutz und Privatheit. 2020 machte er in der Innenstadt von Stuttgart Datenströme über lange Kreidelinien sichtbar. Mehnert entwickelte dazu die Appe Freiheit 2.0, die Bewegungsprofile der Nutzer in Farbbahnen übersetzte.

2013 sorgte er mit den „Waldprotokollen" für Aufsehen: Aus Protest gegen die staatlichen Abhörmaßnahmen US-amerikanischer Geheimdienste und das Tracking von Tech-Konzernen installierte Mehnert Mikrofone in einem Waldstück und veröffentlichte die mitgeschnittenen Gesprächsfetzen von Spaziergängern und Wanderern. *chd*

Einen Bericht über die Arbeit Mehnerts finden Sie in der BvD-News 03/2020, zu der Sie über den QR-Code kommen.

LINK-TIPP

Zentralarchiv der Tätigkeitsberichte der Bundes- und Landesdatenschutzbeauftragten sowie der Aufsichtsbehörden für den Datenschutz

Seit 1971 sammelt das ZafTDA die erschienen Tätigkeitsberichte, aktuell insgesamt 644 Berichte.

▶ www.zaftda.de

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

EFDPO – European Federation of Data Protection Officer

ist ein europäisches Netzwerk nationaler Verbände von Datenschutzbeauftragten. Ihre Aufgabe ist es, eine europäische Interessenvertretung für Datenschutzbeauftragte als Partner von Institutionen wie der Europäischen Kommission, dem Europäischen Parlament, dem Rat der Europäischen Union, dem Europäischen Datenschutzausschuss und den nationalen Datenschutzbehörden aufzubauen. Auf diese Weise will die EFDPO den Datenschutz als Wettbewerbs- und Standortvorteil für Europa stärken.

▶ www.efdpo.eu

ENDSPURT ZUR DAME 2022

Die Bewerbungsphase zur mittlerweile sechsten Runde des Datenschutz Medienpreises (DAME) geht in die Schlussphase. Wichtiges Kriterium, um es unter die Nominierten zu schaffen: Die Arbeiten müssen sich an eine bestimmte Zielgruppe richten und Datenschutz einfach und zugleich anschaulich und konkret erläutern.

Traditionell sind die Gewinner des Vorjahres Mitglied in der aktuellen Jury aus Datenschutzfachleuten und Medienexpertinnen. Den mit 3.000 Euro dotierten DAME-Hauptpreis 2021 holte die Laokoon-Gruppe mit dem Film „Made to Measure – eine digitale Spurensuche“. Gruppenmitglied Hans Block nahm den Preis in Berlin entgegen – und wird nun die Künstlergruppe in der Jury für die DAME 2022 vertreten.

Die Jury, die voraussichtlich im Februar tagen wird, nominiert drei Beiträge. Wer am Ende das Rennen macht erfahren die Nominierten erst bei der Preisverleihung auf den BvD-Verbandstagen am 10. Juni 2023 in Berlin. *chd*

Bis zum **5. Dezember 2022** können sich Medienschaffende, Autorinnen und Journalisten, aber auch Jugendgruppen und Schulklassen mit Videos, Audiobeiträgen, Texten, Clips, Webprojekten oder Songs zu einem Thema rund um den Datenschutz bewerben.

FUTURE LAW

Philipp Reusch (Hrsg.)

Die fortschreitende Entwicklung der Technik im digitalen Umfeld eröffnet viele neue Möglichkeiten für Unternehmen und Behörden. Die Cleveren darunter beziehen dann bei ihren Überlegungen ihre datenschutzrechtliche Beratung mit ein. Doch wer hat schon die Zeit sich neben den Alltagsthemen mit den jeweils neuesten technischen Möglichkeiten und den damit relevanten Fragestellungen entsprechende Lösungsmöglichkeiten zu erarbeiten?

Für dieses Anforderungsprofil will der Band „Future Law" Orientierung und Unterstützung bieten. Schon der Blick ins Inhaltsverzeichnis verrät, wer zur Zielgruppe gehört. Wer sich als Verantwortlicher oder Auftragsverarbeiter mit digitalen Themen und technischen Neuerungen befasst, wird um eine genaue Analyse und Umsetzung regulatorischer Anforderungen nicht umhinkommen. Das Autorenteam einer im Datenschutzrecht bekannten Kanzlei befasst sich in fünf Teilen mit einer allgemeinen Einführung, der Darstellung des rechtlichen Rahmens autonomer Systeme, des „Space Law", digitalen Phänomenen und deren rechtlichen Rahmens sowie abschließend einem Fazit.

Bleiben diese Teile in ihren Bezeichnungen zunächst vielleicht noch etwas nebulös erschließt sich mit dem Blick in deren Unterkapitel der wahre Wert des Werkes: So finden sich in Ausführungen zur außervertraglichen Haftung nach dem Produkthaftungsgesetz, Erläuterungen zur Schaffung einer ePerson und Beschreibungen zum produktsicherheitsrechtlichen Rahmen ebenso wie die Behandlung der Cybersicherheit als Herausforderung. Dabei wird auch die Themenstellung des Verhältnisses von Cybersicherheitsanforderungen zu Geschäftsgeheimnissen und deren angemessener Absicherung angesprochen. Aber auch die Anforderungen bezüglich der Cybersicherheit bei Kritischen Infrastrukturen, IoT-Geräten, Gesundheits-Apps und autonomen Fahrzeugen werden mit einem Ausblick auf eine kommende KI-Verordnung in diesem Kapitel zusammen mit den Erfordernissen für ein Compliance Management zur Cybersicherheit gestreift.

Philipp Reusch (Hrsg.)
Future Law

FACHMEDIEN RECHT UND WIRTSCHAFT IN DEUTSCHER FACHVERLAG GMBH

2. Auflage 2022
234 Seiten
Preis 79,00 Euro
ISBN-13: 978-3800517305

Mehr Raum bekommen die Informationen zum digitalen Upgrade des BGB, welche die Digitale Inhalte-Richtlinie umsetzt. Neben dem neuen Mangelbegriff werden auch datenschutzrechtliche Aspekte beim Bezahlen mit Daten erörtert. Etwas überflüssig erscheint auf den ersten Blick die Darstellung des „Weltraumrechts", bedenkt man aber die Thematik der Zulieferer für Software, Hardware oder Bauteile und die Konsequenzen bei Fehlfunktionen, gibt es doch etliche Fragestellungen, die über das internationale Privatrecht relevant werden und mit dem Titel des Werkes „Future Law" ihre Berechtigung finden. Des Weiteren befasst sich das Werk mit den rechtlichen Fragestellungen des „Digitalen Twins" und der „Blockchain-Technologie" und damit zusammenhängend der Non-Fungible Token (NFT). Die Blockchainthematik wird bezüglich Kryptowährung wie Bitcoin ausführlich beleuchtet. Vertiefte Befassung zu datenschutzrechtlichen Anforderungen erfolgen bei diesem Beispiel nicht. Ein weiteres Beispiel sind Smart Contracts, die als weitere Erscheinungsform von Blockchains beschrieben werden.

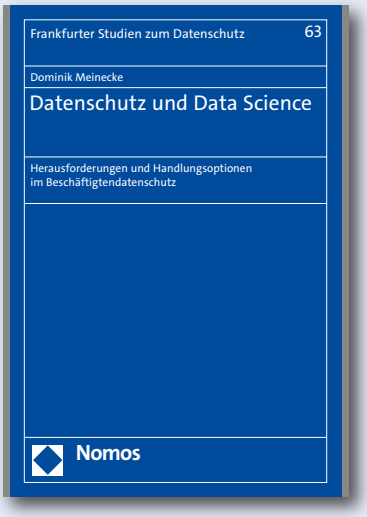
Das Werk ist empfehlenswert für alle diejenigen, die innovative Unternehmen beraten, weil es in kompakter Form einen Überblick über die jeweiligen Thematiken und Fragestellungen liefert und dabei auch noch Lösungsvorschläge anbietet.

Doch entfaltet das Werk auch für Verantwortliche und Auftragsverarbeiter in Kapiteln etwa zur Cybersicherheit oder den BGB-Änderungen seine Relevanz, unabhängig von der technischen Innovationsfreudigkeit. Sein maßgeblicher Vorteil ist für mich die Übersichtlichkeit und Kompaktheit auch komplexer Themen, so dass es sich uneingeschränkt als Einstieg zu den oben geschilderten Fragestellungen empfiehlt.

DATENSCHUTZ UND DATA SCIENCE

HERAUSFORDERUNGEN UND HANDLUNGSOPTIONEN IM BESCHÄFTIGTENDATENSCHUTZ

Dominik Meinecke



Dominik Meinecke
Datenschutz und Data Science" – Herausforderungen und Handlungsoptionen im Beschäftigtendatenschutz

NOMOS VERLAG

1. Auflage 2022
407 Seiten, broschiert
119,00 Euro
ISBN 978-3-8487-8956-6

Das Werk wurde im Rahmen der Dissertation des Autors verfasst. Dementsprechend befasst es sich auch mit strukturellen Erörterungen zum Umgang mit personenbezogenen Daten und der Einordnung gängiger Begrifflichkeiten. Moderne Methoden zur Sammlung und Auswertung großer Datenmengen wie Künstliche Intelligenz, Profiling, automatisierte Entscheidungen oder Big Data wurden unter den Sammelbegriff Data Science betrachtet. Dabei wird die Frage aufgeworfen, ob das aktuelle Datenschutzrecht adäquat mit diesen modernen Methoden der Datenverarbeitung umzugehen vermag und inwieweit Künstliche Intelligenz und maschinelles Lernen damit kompatibel sind. Schon allein diese Fragestellung aus der Einleitung provoziert ein Weiterlesen. Der Autor wählt als Szenario für die Darstellung der Probleme und seiner Lösungsvorschläge den Beschäftigtenkontext. So werden zunächst verwendete Begrifflichkeiten erläutert und dann die Rahmenbedingungen des Art. 88 DS-GVO dargestellt und die Umsetzung in § 26 BDSG bewertet. Einem eigenen Kapitel werden die Verarbeitungsgrundsätze gewidmet – ein Bereich, den auch erfahrene Datenschutzberatende nicht überspringen sollten, werden hier doch die Verständnis- und Interpretationsleitlinien für die Bewertung der Szenarien beschrieben.

Entsprechen der Bedeutung befasst sich der Autor ausführlich mit den Fragestellungen rund um die Einwilligung und Anonymisierung. Bezüglich der Einwilligung begründet er seine Ansicht, dass mehrere Rechtmäßigkeitsgrundlagen parallel verwendet werden können. In einem eigenen Kapitel werden Lösungen und Handlungsempfehlungen erörtert, die sich in Anpassungen der DS-GVO, nationalen Regelungen des Beschäftigtendatenschutzes, datenschutzrechtliche Kollektivvereinbarungen und Ausführungen zu einem Algorithmenrecht unterteilen. Im Ergebnis unterstützt er unter anderem dabei die Forderungen nach gesetzlichen Klarstellungen hinsichtlich der rechtlichen Fragestellungen bei der Einwilligung, bemängelt das Fehlen von Zertifizierungen technischer Standards und empfiehlt die Einbeziehung der Hersteller in die wesentlichen Normen der DS-GVO als Adressaten. Die Erweiterung der Dokumentationspflichten für Verantwortliche und Auftragsverarbeiter könnte Kontrollorganen die Nachvollziehbarkeit erleichtern und die Aufgaben der Aufsichtsbehörden und betrieblichen Datenschutzbeauftragten sollte durch unabhängige Prüfer entlastet werden, die sich am Modell der Wirtschaftsprüfer orientieren könnten. Auf ein eigenes Algorithmenrecht könne verzichtet werden, wohingegen spezifische Produktsicherheitsregelungen wie der diskutierte AI Act begrüßt werden.

Insgesamt ein lesenswertes Buch für alle, die sich mit aktuellen Fragestellungen rund um den Beschäftigtenkontext befassen. Auch wenn ich mir manche Darstellungen etwas stringenter gewünscht hätte, waren mir einige Zusammenhänge und Betrachtungen neu und ich bin gespannt, inwieweit die Ausführungen zu denkbaren Lösungen Eingang in die Rechtsentwicklung finden.

Ergänzend zu dem Thema sei darauf hingewiesen, dass beim EuGH derzeit ein Vorabentscheidungsersuchen bearbeitet wird, das sich mit deutschem Beschäftigtendatenschutz befasst (Az.:C-34/21), das aber aufgrund der zeitlichen Abfolge in dem besprochenen Werk nicht berücksichtigt werden konnte.

IT-SICHERHEIT

TECHNOLOGIEN UND BEST PRACTICES FÜR DIE UMSETZUNG IM UNTERNEHMEN

Michel Lang / Hans Löhr (Hrsg.)

Die beiden Herausgeber sind Professoren an einer Technischen Hochschule und weisen in ihrer Biographie Erfahrungen in der praktischen Umsetzung von Sicherheitsaspekten bei Unternehmen vor. Ihr 16-köpfiges Autorenteam bildet daher ein breites Spektrum an Praktikern ab, die sie dabei unterstützen Grundlagen, Anforderungen und Umsetzung von IT-Sicherheitsmaßnahmen darzustellen.

Das Werk richtet sich an Unternehmen und nimmt sich das Ziel vor Antworten zu geben, wie sich Unternehmen vor Gefährdungen schützen und Sicherheit gewährleisten können. Spezielle Vorkenntnisse werden dabei bei der Leserschaft nicht vorausgesetzt.

Zunächst werden die Gefährdungen und Grundprinzipien zur Gewährleistung der IT-Sicherheit dargestellt. Neben Ausführungen zu Organisationsfragen des IT-Sicherheitsmanagements befassen sich die Autoren mit den rechtlichen Rahmenbedingungen der IT-Sicherheit und skizieren hier die wesentlichen Anforderungen. Nachweismöglichkeiten durch Standards und Zertifizierungen wird ebenso ein eigenes Kapitel gewidmet wie den Ausführungen der Sicherheitsaspekte aus Datenschutzsicht. Erklärungen zu Bedrohungs- und Risikoanalysen ergänzen ebenso wie die Ausführungen zu Reifegradanalysen zu dem IT-Security-Level die Grundlagen. Mit den Aufgaben und Anforderungen an den Chief Information Security Officer (CISO) sowie dessen Möglichkeiten der organisatorischen Einbindung erfahren die Leser wertvoll Hinweise für die Gestaltung organisatorischer Strukturen der IT-Sicherheit.

Die Herausgeber priorisieren die Aspekte der IT-Sicherheit bei der Entwicklung von sicherer Software, in der Produktion, Automotive und intelligenten Gebäuden so, dass sie jeweils ein eigenes Kapitel erhalten. Edge Computing und Sicherheit in der Cloud werden zudem ausführlich behandelt. Zunächst exotisch wirkt das Kapitel, das sich mit der IT-Sicherheit in Vergabeverfahren befasst, doch zeigt sich gerade dabei die Praxisrelevanz des Werkes, berücksichtigt es dabei auch das Geschäftsgeheimnisgesetz bei der Frage, wie im Bieterverfahren mit vertraulichen Informationen umzugehen ist. Den Kapiteln ist ein kurzer Abschnitt vorangestellt, was den Lesenden in diesem Bereich erwartet, manche Kapitel schließen auch mit einer Zusammenfassung und Literaturhinweisen. Komplexere Strukturen werden durch Abbildungen der Abläufe und Zusammenhänge anschaulich vermittelt. Mit dem Werk werden Grundprinzipien gut verständlich, aber auch in der erforderlichen Tiefe dargestellt. Über einen im Buch abgebildeten Zugangscode kann es auch als digitale Fassung durch den Erwerber genutzt werden. In einer künftigen Auflage könnten die weiteren Aspekte des Datenschutzes um das Zusammenspiel mit dem BDSG, aber auch die drohenden finanziellen Risiken, die sich durch immaterielle Schadenersatzforderungen aus Art. 80 DS-GVO ergeben, breiter dargestellt werden, zumal ein Großteil der bisherigen Sanktionen der Aufsichtsbehörden auf Verstößen gegen die Vorgaben der IT-Sicherheit aus Art. 32 DSGO beruhen.

Das Buch empfiehlt sich jedem, der sich neu mit den Anforderungen an die IT-Sicherheit befassen möchte, gibt aber auch erfahreren Datenschutzmitarbeitenden und IT-Security-Experten einen guten Überblick über Anforderungen und die entsprechenden Umsetzungstipps. Zu schätzen ist auch der dafür günstige Preis, der dabei sicherlich unterstützen wird, dass das Buch auch in den verantwortlichen Ebenen aller Unternehmensgrößen Verbreitung finden kann.

Michel Lang / Hans Löhr (Hrsg.)
IT-Sicherheit
Technologien und Best Practices
für die Umsetzung im Unternehmen

CARL HANSER-FACHBUCHVERLAG

1. Auflage 2022
302 Seiten
39,99 Euro
ISBN-978-3-446-47223-5

Rezensionen von

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

MACH DAS INTERNET AUS, ICH MUSS TELEFONIEREN

KURIOSE GESCHICHTEN AUS DER DIGITALEN STEINZEIT

Adrian Lobe

Die Dozenten und Moderatoren erhalten immer ein kleines Dankeschön vom BvD. Auf der Herbstkonferenz & Behördentag im Oktober 2022 in Stuttgart gab es diesmal eine etwas andere Lektüre:

Ach, wie war es doch früher schön. Jedes Land hatte seine eigenen und individuell gestalteten Telefonzellen. Zuhause hatte man die Wahl zwischen apfelgrün und orange und zwischen Wählscheibe oder modernem Tastenfeld. Und der Zugang zu digitaler Kommunikation wurde von lautem Modem-Pfeifen und hohen Kosten begleitet. Der Politikwissenschaftler und Journalist Adrian Lobe veranstaltet in seinem Büchlein „Mach das Internet aus, ich muss telefonieren" eine amüsante Zeitreise in die 90er und frühen 00er Jahre.

Wer etwas über die Entstehungsgeschichte des in den 60er Jahren auf Betreiben des US-Militärs „erfundenen" Internets lernen möchte, wird vom Buch enttäuscht sein. Wer aber das Lebensgefühl der Pubertierenden des zu Ende gehenden 20. Jahrhunderts gerade in Schwaben nacherleben will, ist genau richtig. Das Buch ist witzig und das Lesen macht eine Menge Spaß. Dass Deutschland heute aber weitgehend noch immer in der digitalen Steinzeit lebt, kommt leider zu kurz. Das Buch endet leider genau da, wo es spannend wird. Die gesellschaftlichen und politischen Umbrüche durch das Internet, durch Twitter, Facebook, LinkedIn, etc. spielen in der Zeit nach dem Buch. Die Leser dürfen auf eine Fortsetzung gespannt sein.

Und wer genug davon hat, dem Autor in seine Jungend im Schwabenland zu folgen, wird die Anmerkungen am Ende des Buches lieben. Zu jedem Kapitel gibt es eine Fülle an Web-Adressen, um selbst tiefer zu recherchieren, um nachzulesen und sich gezielt zu informieren. Ein Buch, das Spaß macht und zum Weiter-Denken anregt.

Adrian Lobe
Mach das Internet aus, ich muss telefonieren
Kuriose Geschichten aus der digitalen Steinzeit

C.H.BECK

2022
192 Seiten, Paperback
12,95 Euro
ISBN: 978 3 406 79116 1

Rezension von

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

▶ www.AdOrgaSolutions.de

ÜBERBLICK

REZENSIONEN 2022

Titel	Autor	Verlag	Jahr	Erschienen in
MEINE AUFGABEN ALS DATENSCHUTZBEAUFTRAGTER	Rudi Kramer	C.H. Beck	2022	BvD-News 1/22
TTDSG LEICHT ERKLÄRT	Dr. Jens Eckhardt	PrivacyExpert	2021	BvD-News 1/22
DATENSCHUTZ IM UNTERNEHMEN	Michael Wächter	C.H. Beck	2021	BvD-News 1/22
KÜNSTLICHE INTELLIGENZ	Dr. Kuuva Josef Chibanguza, Christian Kuß, Hans Steege (Hrsg.)	Nomos	2022	BvD-News 1/22
HEIDELBERGER KOMMENTAR ZUM TTDSG	Prof. Dr. Rolf Schwartmann, Andreas Jaspers, Dr. Jens Eckhardt (Hrsg.)	C.F. Müller	2022	BvD-News 2/22
FORMUILARHANDBUCH DATENSCHUTZRECHT	Dr. Ansgar Koreng, Dr. Matthias Lachenmann (Hrsg.)	C.H. Beck	2021	BvD-News 2/22
DATENSCHUTZRECHT	Annika Selzer (Hrsg.)	Fraunhofer Verlag	2022	BvD-News 2/22
PRAXISHANDBUCH KÜNSTLICHE INTELLIGENZ	Lothar Schröder, Petra Höfers	Bund Verlag	2022	BvD-News 2/22
FUTURE LAW	Philipp Reusch (Hrsg.)	Deutscher Fachverlag	2022	BvD-News 3/22
IT-SICHERHEIT	Michel Lang, Hans Löhr (Hrsg.)	Hanser Fachbuch	2022	BvD-News 3/22
MACH DAS INTERNET AUS, ICH MUSS TELEFONIEREN	Adrian Lobe	C.H. Beck	2022	BvD-News 3/22
DATENSCHUTZ UND DATA SCIENCE	Dominik Meinecke	Nomos	2022	BvD-News 3/22

BvD-Webinare & Online-Seminare

BvD e.V.
DATENSCHUTZ GESTALTEN

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Termin	Thema
12.12.2022	**BvD-Blitzlicht – Information zur Verhaltensregel** „Trusted Data Processor“
20.12.2022	**Webinar – Praktische Umsetzung der Verhaltensregel** „Trusted Data Processor“
12.01.2023	**Webinar – Praktische Umsetzung der Verhaltensregel** „Trusted Data Processor“
25.01.2023	**Webinar – Praktische Umsetzung der Verhaltensregel** „Trusted Data Processor“
26.01.2023	**Webinar – Privacy Litigation aus der Sicht des DSB: Einordnung und Umgang mit Schadensersatzansprüchen**
23.02.2023	**Webinar – MS365 – was geht und was nicht?**
21. – 23.03.2023	**Online-Seminar – Get Ready: Datenschutz für Koordinatoren**
22. – 23.03.2023	**Online-Seminar & Workshop – IT für Datenschutzbeauftragte**

BvD-Veranstaltungen

09.-10.05.2023	**BvD-Verbandstage 2023** Berlin
05.07.2023	**2. Datenschutztag Hessen & Rheinland-Pfalz** Frankfurt/Main
18. – 20.10.2023	**BvD-Herbstkonferenz & Behördentag** München

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

Die wichtigsten Daten der BvD-Gremien

Detaillierte Informationen zu den Treffen und Terminen finden Sie unter:

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

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

19.01.2023	RG Mitte	**17.02.2023**	RG Nürnberg
26. – 28.01.2023	AK Externe	**23.02.2023**	RG Nord
30.01.2023	AK Krypto	**30.03.2023**	RG Mitte
07.02.2023	RG West	**12.04.2023**	RG Sachsen
10.02.2023	RG Stuttgart		

Bitte beachten Sie:

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

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

Termine und Anmeldung finden Sie auf unserer Webseite:

- www.bvdnet.de/termine/

BVD-STELLENBÖRSE

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

- www.bvdnet.de/bvd-stellenboerse

VERNETZEN SIE SICH MIT UNS:

- www.bvdnet.de

XING: www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

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

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

RSS-Feed: www.bvdnet.de/feed/

BVD PARTNERSHIP PROGRAM

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

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

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

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

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

Wir danken unseren Silver Partnern:

OneTrust PRIVACY, SECURITY & GOVERNANCE — RHENUS OFFICE SYSTEMS

▶ www.onetrust.de ▶ www.rhenus.group/de

WEITERE WICHTIGE KONTAKTE

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

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

Marketing

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

Wettbewerb

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

Schulprojekt

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

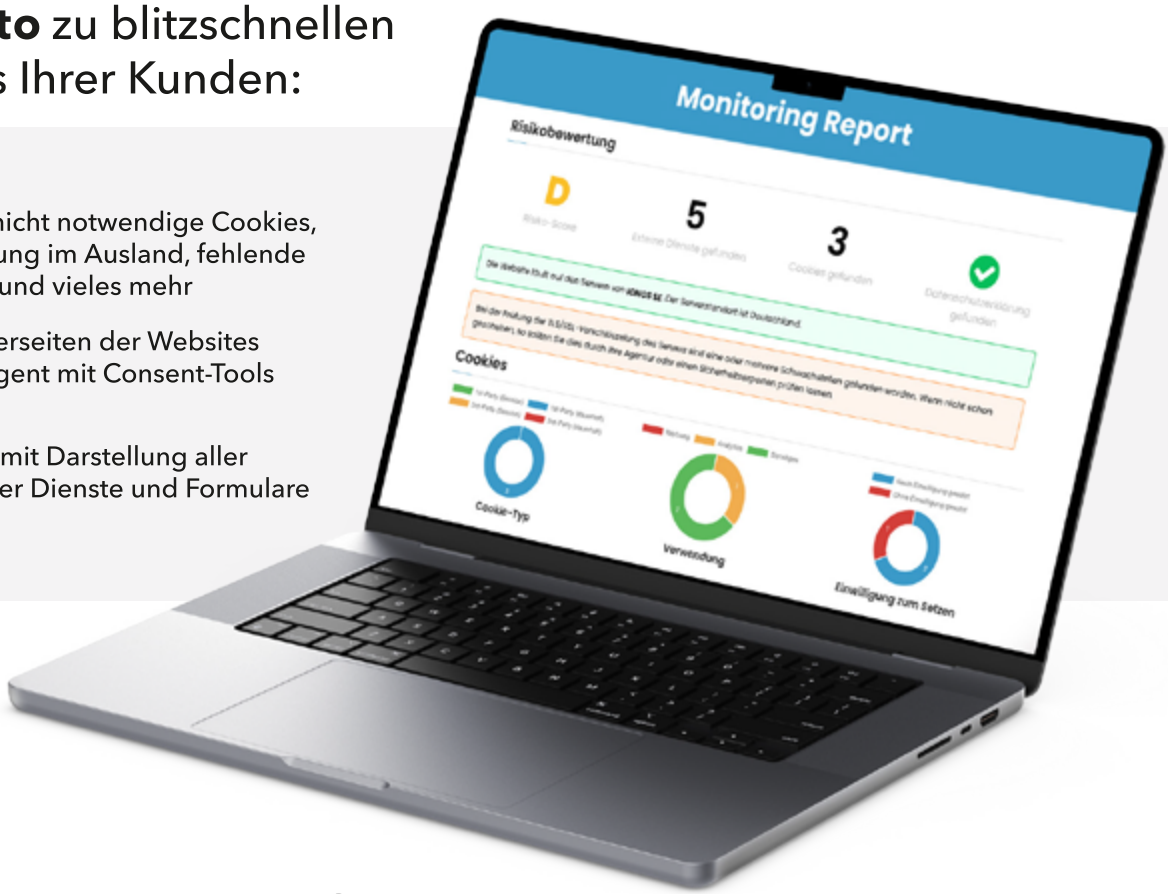
privacy4people POWERED BY BvD
privacy4people - Gesellschaft zur Förderung des Datenschutzes gGmbH
IHRE SPENDE FÜR DEN DATENSCHUTZ:
Commerzbank
IBAN: DE 30 5054 0028 0424 5577 00
BIC: COBADEFFXXX
Telefon: +49 30 20 62 14 41
mail@privacy4people.de • www.privacy4people.de

Anzeige

Websites manuell auf Datenschutzlücken zu durchsuchen ist Vergangenheit!

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

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



Sind Sie bereit dafür, Ihre Zeit besser zu nutzen?

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

decareto

Alle Informationen finden Sie auf **www.decareto.de**
Vereinbaren Sie noch heute einen **Beratungstermin** unter **0177 3415205**
oder besuchen Sie unsere Website für eine **kostenfreie 14-Tage-Testphase**.