Ausgabe 02/2019

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Künstliche Intelligenz trifft Datenschutz

Der digitale Wandel unserer Gesellschaft

DATENSCHUTZ BEI KÜNSTLICHER INTELLIGENZ – S.5

EIN JAHR DSGVO – S.28

WIE KANN MAN SECURITY AWARENESS MESSEN UND TRAINIEREN? – S.68

30 JAHRE BVD – FÜNF FRAGEN AN... – S.72

BvD e.V.

DATENSCHUTZ GESTALTEN

Anzeige

Ausblick

Seminare – 2. Halbjahr 2019

Termin	Thema	Ort
05.09.2019	**Artikel 26 DSGVO – Die gemeinsame Verantwortlichkeit**	Nürnberg
01.10.2019	**Internationaler Datenschutz**	Nürnberg
11.10.2019	**BvD-Newcomerforum**	München
14.10.2019	**Beschäftigtendatenschutz - Seminar**	Frankfurt/Main
15.10.2019	**Beschäftigtendatenschutz - Workshop**	Frankfurt/Main
18.10.2019	**DSK zum Direktmarketing: Das müssen Sie beachten!**	Hamburg
22.10.2019	**Die ePrivacy-Verordnung**	Nürnberg
22.10.2019	**Umsetzung der DSGVO – Von der Panik zum Tagesgeschäft – Schwerpunkt Betroffenenrechte, Informationspflichten**	Nürnberg
25.11.2019	**Verzeichnis der Verarbeitungstätigkeiten und Dokumentation**	Frankfurt/Main
28.11.2019	**BvD-Expertenforum mit drei ausgewählten Themen**	Düsseldorf
12.12.2019	**Datenschutzverletzungen, Prüfungen, Bußgeld**	Düsseldorf

* für BvD-Mitglieder

Information und Anmeldung unter www.bvdnet.de

DIGITALISIERUNG UND KÜNSTLICHE INTELLIGENZ

Liebe Leserinnen und Leser,

Digitalisierung und Künstliche Intelligenz zählen zu den aktuellen großen Trends und bestimmen die politische Agenda in Deutschland. Auch in der Wirtschaft geht kein Weg an den Themen vorbei. Allerdings wird unter diesen Buzzwords häufig auch nur „alter Wein in neuen Schläuchen“ angeboten. Schaut man hinter die schicke Fassade, finden sich alte Produkte, die mit selbstlernenden Systemen so gar nichts zu tun haben. Während die politische Öffentlichkeit i.d.R. nicht das Know-how besitzt dies zu erkennen und entsprechend kritischer damit umzugehen, sollten Datenschutzbeauftragte durchaus in der Lage sein anhand der entsprechenden Informationen zu erkennen, welche Technologie im Einsatz ist und welches Risiko diese für die betroffenen Personen darstellt.

Im medizinischen Bereich beispielsweise könnte KI-Systemen schon in wenigen Jahren der Durchbruch gelingen und zu besseren Ergebnissen führen. Ein Bewerber-Eignungstest allerdings, der anhand einer Stimmanalyse erkennen will, ob der Bewerber für einen Job geeignet ist, gehört bislang nicht zu den selbstlernenden Systemen – auch wenn es so beworben wird. Aufgrund der fragwürden Analysemethode und der Intransparenz kann dieser für die Bewerber sehr leicht zu einem Risiko werden.

Die BvD-Verbandstage haben sich daher in diesem Jahr ausführlich mit KI-Systemen befasst. In vielen Beiträgen haben die zahlreichen Referenten die verschiednen Aspekte der Technologie beleuchtet. Der BvD wird das Thema auch bei den Fortbildungen weiter auf der Agenda haben, um Sie mit dem erforderlichen Know-how auszustatten.

Know-how und Erfahrung sind die Schlüssel bei der Umsetzung der Anforderungen aus der DSGVO. Die Unternehmen, vor allem wenn nur noch wenige Mitarbeiter mittels digitalisierter Prozesse oder gar KI-Systemen personenbezogene Daten verarbeiten, müssen sich mit den Anforderungen auseinandersetzen. Die Anzahl der Mitarbeiter spielt dabei kaum eine Rolle mehr. Heute reichen wenige Mitarbeiter, um Millionen von Datensätzen zu verarbeiten. Aus diesem Grund ist die Erhöhung der Benennungsgrenze von 10 auf 20 Personen genau der falsche Schritt.

Es geht hier gar nicht um den vielbemühten Handwerker – der ist i.d.R. gar nicht von der Benennungspflicht betroffen. Es geht um die zahlreichen Dienstleister, die Daten im großen Umfang verarbeiten und dazu nur wenige Mitarbeiter benötigen. Hier müssen wirksame Maßnahmen die betroffenen Personen schützen – und hier hat sich die Funktion des betrieblichen Datenschutzbeauftragten seit Beginn der Digitalisierung vor über 40 Jahren bewährt und gehört untrennbar dazu. Der BvD wird sich auch in Zukunft dafür einsetzen, dieses bewährte Modell weiter zu entwickeln.

Viel Spaß bei der Lektüre!

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

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

Redaktion:
Thomas Spaeing
(V.i.S.d.P., bvd-news@bvdnet.de)
Katrin Eggert

Fotos:
123rf.com

Lektorat:
Frank Spaeing, Regina Mühlich

Anzeigen:
Katrin Eggert
(bvd-gs@bvdnet.de)

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

ISSN: 2194-1025
Erscheinungsweise: 3 × jährlich, ca. 4.000 Exemplare
(Mediadaten anfordern unter 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.

EDITORIAL

Digitalisierung und Künstliche Intelligenz – *Thomas Spaeing* 3

KI & DATENSCHUTZ

Datenschutz bei Künstlicher Intelligenz – *Prof. Dr. Dieter Kugelmann* 5
Kein blindes Vertrauen – Ein Plädoyer für mehr menschliche Kompetenz in der algorithmischen Gesellschaft – *Jörg Dräger und Ralph Müller-Eiselt* 9
Algorithmenbasierte Entscheidungssysteme: Vertrauen ist gut – Kontrolle ist besser – *Dr. Miika Blinn, Florian Glatzner* 13
Datenschutz-Folgenabschätzung gemäß ISO 29134 im Rahmen der Entwicklung einer KI-Anwendung – *Beate Beißwenger und Volker Ibisch* 18
KI im Anwendungsfeld der Fraud Prevention – *Prof. Dr. Oliver Weissmann und Mirjam H. Steinfeld, Mag iur.* 24

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Ein Jahr DSGVO – *Interview* mit Dr. Stefan Brink 28

GESETZESÄNDERUNG

EU-Staaten beschließen neues Urheberrecht – *Nils Steffen* 30

DATENSCHUTZPRAXIS

Ihnen steht ein Update für Ihre datenschutzrechtliche Einwilligung zur Verfügung! – *Dr. Carlo Piltz und Melanie Pradel* 32
Datenschutz im Unternehmen: Cloud vs. On-Premise – *Philip Kissi* 36
Interview mit dem Fraunhofer-Institut für sichere Informationstechnologie zum Thema „Volksverschlüsselung" – *Michael Herfert und Jürgen Hartz* 40
Arbeit 4.0 – Die Digitalisierung der Arbeitswelt – *Regina Mühlich* 44
Artikel zum neuen Californischen Datenschutz Gesetz – *Jutta Oberlin* 47
Gesunder Datenschutz – *Prof. Dr. Lothar Determann* 54

AUFSICHTSBEHÖRDEN

Erste Prüfungen im Rahmen der DSGVO – die Querschnittsprüfung der LfD Niedersachsen – *Barbara Thiel* 60
Ein Schritt zur verbesserten Transparenz für alle – der „Datenschutz-Steckbrief" – *Marit Hansen und Angelika Martin* 64

GESELLSCHAFT

Wie kann man Security Awareness messen und trainieren? Einblick in den »Faktor Mensch« in der IT-Sicherheit – *Anjuli Franz* 68

AUS DEM VERBAND

30 Jahre BvD – Fünf Fragen an... 72
Gründung der European Federation of Data Protection Officers (EFDPO) in Berlin – *Regina Mühlich und Thomas Spaeing* 78
DAME-Gala: Mit der Glitterkanone auf die Gewinner. Zweiter Datenschutz Medienpreis bringt Rhythmus und Emotionen in die Verbandstage 2019 80

REZENSIONEN

Handbuch Europäisches und deutsches Datenschutzrecht – *Prof. Dr. Louisa Specht und Dr. Reto Mantz* 83
IT-Outsourcing und Cloud-Computing – *Peter Bräutigam (Hrsg.)* 84
Betrieblicher Datenschutz – *Forgó / Helfrich / Schneider* 85
Datenschutz im Gesundheitswesen – *Benedikt Buchner (Hrsg.)* 86
Datenschutzrecht für Schweizer Unternehmen – DSGVO – *Benjamin Domenig, Christian Mitscherlich* 87
Die Optimierer – *Theresa Hannig* 88

TERMINE UND KONTAKTE

Überblick Seminare und Workshops 2019 89
Termine der Regionalgruppen und Arbeitskreise des BvD 90

DATENSCHUTZ BEI KÜNSTLICHER INTELLIGENZ

Prof. Dr. Dieter Kugelmann

Das Thema Künstliche Intelligenz (KI) ist in aller Munde. Allerdings fehlt es an einem allgemein anerkannten Verständnis von KI. Dies verwundert nicht, weil KI-Systeme äußerst vielgestaltig sind und eine große Bandbreite an Ausgestaltungen und Einsatzmöglichkeiten besitzen. KI hat Big Data als Modebegriff und Platzhalter für moderne und innovative Datenverarbeitung abgelöst, ohne dass alle rechtlichen Fragen beantwortet sind, die sich bereits bei der Anwendung von Big Data Lösungen gestellt haben. Jedoch ist nicht jede Datenverarbeitung schon deshalb modern und innovativ, weil sie auf dem Einsatz von KI-Systemen beruht. Gesellschaftlich akzeptierte und rechtlich zulässige Datenverarbeitungen sollten zukunftsorientierte informationstechnische Lösungen mit einem hohen Standard an Datenschutz und Informationssicherheit verbinden.

Bei dem Einsatz von KI-Systemen geht es um die Verwendung von Algorithmen, die regelmäßig in Anwendungen eingesetzt werden, die mit Big Data arbeiten. Algorithmen prägen bekanntermaßen unseren Alltag bereits seit längerem in erheblichem Maße. Algorithmen selbst sind weder gut noch schlecht, sie sind lediglich nützlich oder weniger nützlich. Und sie sind von Menschen geschaffen. Algorithmen benötigen Daten und sie verarbeiten sie. Datenverarbeitung geschieht aber nicht im rechtsfreien Raum. Der Einsatz von KI-Systemen ist am Datenschutzrecht zu messen.

Im Jahr 2019 hat Rheinland-Pfalz den Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) inne und hat das Jahr 2019 unter das Leitthema ▸

KI & DATENSCHUTZ

KI gestellt. Unter Leitung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz wurde eine Task Force KI ins Leben gerufen, die zunächst eine Grundsatzerklärung zu Datenschutz und KI ausgearbeitet hat. Auf der Konferenz der DSK auf dem Hambacher Schloss am 3. und 4. April 2019 wurde die Hambacher Erklärung eingehend diskutiert, modifiziert und dann verabschiedet.

Die Hambacher Erklärung zur Künstlichen Intelligenz ist als Grundsatzpapier gedacht, das dem Datenschutzrecht verpflichtet ist. Der DSK geht es in der Erklärung darum, die rechtlichen Anforderungen an den Einsatz von KI-Systemen herauszuarbeiten und aus datenschutzrechtlicher Sicht die Entwicklung zu begleiten. Ohne Zweifel spielen technische, ethische und gesellschaftliche Aspekte eine erhebliche Rolle im Zusammenhang der Entwicklung von Systemen und des Einsatzes Künstlicher Intelligenz. Die DSK hat jedoch ausdrücklich einen rechtlichen Ansatz gewählt, um deutlich zu machen, dass es insoweit auf der Grundlage der Datenschutz-Grundverordnung bereits rechtliche Anforderungen an den Einsatz von KI-Systemen gibt.

Ausgangspunkt ist dabei die Wahrung der Grundrechte. Der Grundrechtsschutz und insbesondere auch der Datenschutz müssen mit aktuellen Entwicklungen Schritt halten, um nicht erst im Nachgang Grenzen zu ziehen, sondern schon die Entwicklung konstruktiv begleiten zu können. Vor dem Hintergrund Künstlicher Intelligenz ist das deshalb nicht einfach, weil es keine anerkannte Definition gibt. Die DSK hat sich auf die Definition der Bundesregierung in deren KI-Strategie gestützt. Allerdings hat bereits die Datenethik-Kommission der Bundesregierung diese Definition weiter ausdifferenziert. Sicherlich sind hier noch weitere Fortentwicklungen, Differenzierungen und Konkretisierungen möglich und erforderlich. Algorithmen und darüber hinaus selbstlernende Systeme werden zunehmend eingesetzt. Immerhin ist festzustellen, dass die Entwicklung an einigen Punkten doch noch am Anfang steht. Auch wenn vielfach mit dem schillernden Begriff der Künstlichen Intelligenz argumentiert wird, bedarf es doch sehr genauer Betrachtung, um was es sich genau handelt. Nicht jeder Spam-Filter, der algorithmenbasiert arbeitet, birgt erhebliche Gefahren für die Grundrechte. Im Falle von KI-Systemen, die etwa die Bewerberauswahl in großen Bewerbungsverfahren unterstützen, kann dies durchaus anders sein. Erst recht sind KI-Systeme besonderer Betrachtung würdig, wenn es um Daten besonderer Kategorien i.S.d. Art. 9 DSGVO wie Gesundheitsdaten geht. Apps im Gesundheitswesen, die vielleicht sogar selbstlernende Aspekte beinhalten, können erhebliche rechtliche und vor allem auch praktische Auswirkungen haben.

In der Hambacher Erklärung hat die DSK hervorgehoben, dass KI Menschen nicht zum Objekt machen darf. Die Menschenwürde ist unantastbar und auch bei dem Einsatz von KI-Systemen das Leitbild. Hier liegt ein wesentliches Einfallstor für ethische Wertungen. Auch im digitalen Zeitalter bilden die Würde des Menschen und das Demokratieprinzip zentrale Maßstäbe staatlichen und wirtschaftlichen Handelns. Grundrechte gelten selbstverständlich auch im Zusammenhang mit Künstlicher Intelligenz. Die Grundrechte sichern Freiheit und Gleichheit gegenüber dem Staat und sie sichern die Ausübung von Freiheit in der Gesellschaft. Der Staat hat einen Schutzauftrag, den er erfüllen muss. Dabei geht es keineswegs darum, Entwicklungen zu ersticken, sondern Rahmenbedingungen zu entwickeln, auch um die Akzeptanz für den Einsatz von KI-Systemen bei den Bürgern zu unterstützen. Die verfassungsrechtlichen Grundsätze finden teils ihren Niederschlag in konkreten einfachrechtlichen Anforderungen, die insbesondere in der Datenschutz-Grundverordnung zu finden sind.

Die Datenschutz-Grundverordnung enthält eine Reihe von allgemeinen Prinzipien, die fruchtbar gemacht werden können. Dabei ist zwischen der Entwicklung von KI-Systemen und ihrem Einsatz zu unterscheiden. Für die Entwicklung gelten andere Maßstäbe, weil insoweit die Wissenschaftsfreiheit eine Rolle spielen kann. Nichts desto trotz ist auch bei der Forschung auf die Einhaltung der Vorgaben der DSGVO zu achten, wenn personenbezogene Daten verwendet werden. Wenn und soweit anonymisierte Daten als Trainingsdaten für die Entwicklung des KI-Systems nutzbar gemacht werden können, entfallen eine Reihe von Problemen.

Beim Einsatz von KI-Systemen sind die Anforderungen höher als bei der Forschung unter Laborbedingungen. Es geht auch darum, dass der für den Einsatz Verantwortliche für die Sicherstellung der rechtlichen Vereinbarkeit des KI-Systems Verantwortung trägt. Zu beachten ist, dass nach Art. 25 DSGVO dem Verantwortlichen auch die Verpflichtung für den Datenschutz by design auferlegt ist. Er wird sinnvoller Weise nur Systeme erwerben, die entsprechenden Kriterien entsprechen. Die Entwickler werden daher die Anforderungen des Datenschutzes an den Einsatz eines KI-Systems im Blick behalten, wenn sie ein Produkt letztlich zur Einsatzreife bringen wollen.

Rechtliche Anforderungen sind etwa die Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO oder die Einhaltung des Grundsatzes der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO. Technische und organisatorische Standards sind noch weiter zu entwickeln. Sie sind jedenfalls nach Art. 24 und 25 DSGVO notwendig und können Fragen der Pseudonymisierung und Anonymisierung betreffen.

Von erheblicher Bedeutung ist der Grundsatz, wonach personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen (Art. 5 Abs. 1 lit. a DSGVO). Nachvollziehbarkeit und Erklärbarkeit sind wesentliche Aspekte beim Einsatz von KI-Systemen. Dies hat auch die Internationale Konferenz der Datenschutz- und Privatheitsbehörden (ICDPPC) in einer Resolution festgehalten. Nichts desto trotz bedarf es weiterer Ausschärfung, was der rechtliche Begriff der Nachvollziehbarkeit hier technisch bedeuten kann. An dieser Stelle wird die DSK weiter arbeiten. Jedenfalls ist klar, dass Erklärbarkeit gewährleistet sein muss. Dies ist Aufgabe der Verantwortlichen, die KI-Systeme einsetzen. Nur dann können Diskriminierungen vermieden werden. Es geht auch um Intervenierbarkeit. Wenn ein selbstlernendes System, wenn neuronale Netze insoweit eigenständig Datenverarbeitungen vornehmen, muss sichergestellt sein, dass ein Eingreifen des Menschen möglich ist und auch noch rechtzeitig kommen kann, um Datenschutzverletzungen zu verhindern.

Die Task Force KI der DSK beschäftigt sich weiter mit dem Thema und beabsichtigt, einige ausgewählte konkrete Aspekte näher zu erarbeiten. Es soll darum gehen, in bestimmten Anwendungsfeldern den Verantwortlichen Hilfestellung zu leisten, wenn es um die datenschutzkonforme Anwendung von KI-Systemen geht. Dazu können übergeordnete Gesichtspunkte aus informationstechnischer Sicht einen wesentlichen Beitrag leisten. Die DSK verfolgt damit weiter ihren konstruktiven Ansatz, der Innovationen möglich machen und zugleich Grundrechte sichern soll.

Es gibt keinen Grund, vor der Entwicklung zu kapitulieren. Dazu ist diese Entwicklung auch viel zu vielfältig und unabsehbar. Die Entwicklung von KI-Systemen wird sicherlich Auswirkungen auf die Arbeit der Zukunft, auf das Gesundheitswesen oder die Mobilität haben. Hier gilt es, positive Wirkungen zu fördern und Nachteile möglichst auszuschließen. Nachteile sind auch Verletzungen des Datenschutzrechts. Es ist Aufgabe der Datenschutzaufsichtsbehörden, die Rechtmäßigkeit von Datenverarbeitungen zu prüfen. Daher bedarf es des Blickes auf aktuelle Entwicklungen, um diese aufsichtsbehördliche Aufgabe effektiv und sinnvoll zu erfüllen.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder wollen ihren Beitrag leisten. Darüber hinaus sind selbstverständlich ethische und gesellschaftliche Diskussionen dringend erforderlich, um im Hinblick auf spezifische Einsatzfelder Vorteile und Nachteile von KI-Systemen abzuwägen. Die Frage, ob hier gesetzgeberische Regelungen möglich und sinnvoll sind, kann nur vor dem Hintergrund beantwortet werden, ob und wie die Gesellschaft bestimmte Entwicklungen für sinnvoll hält. Das Datenschutzrecht als solches gilt bereits. Aber auch insoweit sind durchaus Weiterentwicklungen denkbar. Dies kann etwa den Art. 22 DSGVO zur automatisierten Datenverarbeitung betreffen. In konkreten Zusammenhängen sind die besonderen Gegebenheiten des Einsatzes von KI-Systemen zu berücksichtigen. Dies gilt etwa für Datenschutz-Folgenabschätzungen, wenn komplexe Datenverarbeitungen bewertet werden müssen. Die Einschätzung von Risiken, die durch Datenverarbeitung hervorgerufen werden, wird wesentlich auch davon beeinflusst, ob ein simpler Algorithmus oder aber ein komplexes ▸

neuronales Netz zum Einsatz kommen. Vor diesem Hintergrund bedarf es einer möglichst spezifischen Einschätzung bestimmter Datenverarbeitungen. Bewertungen des Einsatzes von KI-Systemen müssen zwar auf möglichst breiter und solider Grundlage getroffen werden, die etwa durch Wertungen des Gesetzgebers oder Gremien der Ethik vorgegeben werden kann. Allerdings ist es wenig nützlich, ausufernde Betrachtungen im Einzelfall vorzunehmen. Die Wissenschaft betreibt teils in Kooperation mit der Wirtschaft Grundlagenforschung, um für die Gestaltung und Beurteilung von KI-Systemen dann handhabbare Kriterien zur Verfügung zu stellen.

Ethische und weitere Grundsätze von übergeordnetem Charakter spielen bei Auslegungen des Datenschutzrechts eine Rolle. Daher sind nicht nur die Gesetzgeber auf europäischer und innerstaatlicher Ebene gefordert, sich mit diesen Fragen auseinander zu setzen, sondern auch die Behörden, die entsprechende Verarbeitungen zu beurteilen haben. Diese Herausforderung anzunehmen setzt voraus, dass grundlegende Richtungsentscheidungen und wesentliche Feststellungen getroffen werden. Hier hat sich die DSK in ihrem Aufgabenbereich auf den Weg gemacht. Mit der Hambacher Erklärung liegt ein Grundsatzdokument vor, auf dessen Basis weitere Überlegungen getroffen werden können und müssen. Dieser Weg soll und wird weiter intensiv und konstruktiv verfolgt werden.

Die Datenschutzaufsichtsbehörden können in der Anwendung des Datenschutzrechts und der Beratung bei dem Einsatz von KI-Systemen ihren Beitrag leisten. In der Demokratie ist es aber die vornehmste Aufgabe des Gesetzgebers, die Freiheit und Gleichheit der Bürgerinnen und Bürger zu gewährleisten. Er muss die wesentlichen Rahmenbedingungen für die Entwicklung und den Einsatz von KI-Systemen festlegen. Die DSGVO bietet eine gute rechtliche Grundlage, auf die weitere Regelungen aufbauen können. Das stete Bemühen um Fortschritt zum Wohl der Menschen geht einher mit dem steten Ringen um Freiheit in der Demokratie.

Über den Autor

Prof. Dr. Dieter Kugelmann
Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Anzeige

KI & DATENSCHUTZ

KEIN BLINDES VERTRAUEN – EIN PLÄDOYER FÜR MEHR MENSCHLICHE KOMPETENZ IN DER ALGORITHMISCHEN GESELLSCHAFT

Jörg Dräger und Ralph Müller-Eiselt

Algorithmen und Künstliche Intelligenz verheißen Beeindruckendes: eine gerechtere, sicherere und effizientere Welt. Sie können weniger diskriminierend als ein Richter bewerten, ob jemand ins Gefängnis gehört oder nicht. Sie schicken die Polizei dorthin, wo wahrscheinlich bald ein Verbrechen geschieht. Und sie lösen Aufgaben, die für uns Menschen zu komplex sind, beispielsweise zehntausende Schüler ihren Wünschen entsprechend auf hunderte weiterführende Schulen verteilen. Das ist keine Science-Fiction, sondern in Städten wie New York City längst Alltag. Moderne Technologie soll dort der Schlüssel zu einer besseren Gesellschaft sein. Für den Einzelnen kann das aber auch handfeste Nachteile haben.

In Australien etwa verweigert der automatisierte Sprachtest einer Muttersprachlerin wegen mangelnder Englischkenntnisse die Einwanderungserlaubnis; er kennt ihren irischen Akzent nicht. Ein Algorithmus in Florida empfiehlt einem Richter, ein 18-jähriges Mädchen nach einem Fahrraddiebstahl in den Knast zu stecken – und lässt einen mehrfach verurteilten Räuber in Freiheit. Ein Grund: die Hautfarbe. Die Software von Autoversicherungen bietet solventen Verkehrsrowdys in den USA günstigere Tarife an als tadellosen Fahrern mit niedriger Kreditwürdigkeit. Auch das ist Realität in der künstlich intelligenten Gesellschaft: Algorithmen setzen den größten Unfug mit maschineller Präzision um.

Unsere Verantwortung

Verantwortlich für deren Versagen sind wir Menschen. Wir definieren ihre Ziele, wir programmieren ihren Code, wir entscheiden über ihren Einsatz. Deshalb sollten wir auch ihre Wirkung kontrollieren. Das erfordert mehr algorithmische Kompetenz und bedeutet mehr ethische Verantwortung: Bei Programmierern, die Software erschaffen. Bei Anwendern, die sie nutzen. Und bei Führungskräften, die sie für ihr Unternehmen oder den Staat beauftragen.

Programmierer kommen immer öfter in Situationen, in denen ein moralischer Kompass unverzichtbar ist. Die ▸

KI & DATENSCHUTZ

Diesel-Abschalteinrichtung ist nur ein Beispiel: Ist es verwerflich, eine Software zu programmieren, die feststellt, ob sich ein Auto auf der Straße oder auf dem Prüfstand befindet? Wenn man die böse Absicht dahinter kennt: natürlich. Nur so war es den Autoherstellern möglich, die Abgasnormen zu umgehen.

Auch professionelle Nutzer müssen Algorithmen kompetent und reflektiert anwenden. Oft handelt es sich um Assistenzsysteme: Am Ende steht ein Arzt, Richter oder Polizist, der ihre Empfehlungen interpretiert und dann eine Entscheidung fällt. Das Vertrauen in den Computer ist dabei häufig groß. Doch wenn diese Anwender die Ziele und Wirkungsweise der Technologie nicht kennen, schleichen sich Fehler ein. Die Chicagoer Polizei etwa hat in ihrer täglichen Arbeit eine Software nicht wie vorgesehen zur Prävention, sondern zu Ermittlungszwecken genutzt. Potenzielle Verbrechensopfer wurden so zu Verdächtigen gemacht. Der Algorithmus funktionierte, wurde aber falsch eingesetzt.

Noch kokettieren manche Führungskräfte mit fehlendem Technologie-Verständnis. Dabei ist es verantwortungslos, wenn die Personalchefin eines großen US-Unternehmens sagt, sie wisse nicht, warum ihre Software zur Bewerberauswahl funktioniere, sondern nur, dass sie funktioniere und die Zahl der Kündigungen zurückgehe. Es ist vielmehr Teil moderner Führungsverantwortung, ethisch vertretbare Algorithmen zu garantieren. Das bedeutet auch, bei vermeintlich guten Ergebnissen zu prüfen, wie sie zustande kommen und ob sie Nebenwirkungen haben. In diesem konkreten Fall eine soziale und ethnische Diskriminierung: Das automatisierte Verfahren bevorzugte Mitarbeiter mit kurzem Arbeitsweg, die dem Unternehmen zwar länger die Treue hielten, benachteiligte aber diejenigen Bevölkerungsgruppen, die sich die höheren Wohnkosten rund um die Firmensitze nicht leisten konnten.

Mehr Kompetenz

Nur wer versteht, wie die eigenen Systeme arbeiten, kann Fehler und Probleme entdecken – und abstellen. Wo Maschinen Menschen bewerten und das Urteil von hoher Tragweite ist, müssen wir dessen Kriterien diskutieren und definieren. Warum kommt der eine Schüler auf seine Wunschschule und der andere nicht? Warum kontrolliert die Polizei in dem einen Bezirk häufiger als in dem anderen? Wir tragen die gesellschaftliche Verantwortung dafür, dass Software, die unser Leben bestimmt, richtig funktioniert und andernfalls so korrigiert wird, dass sie ihren Zweck angemessen erfüllt.

Wenn das nicht möglich ist, dürfen wir vor Verboten nicht zurückschrecken. Auch die künstliche Verdummung künstlicher Intelligenz (KI) ist in einer Demokratie ein legitimes Mittel: Nicht alles technisch Machbare ist gesellschaftlich wünschenswert oder akzeptabel. Damit Maschinen den Menschen dienen, sollten wir nicht nur in die Künstliche Intelligenz der Maschinen, sondern auch in die algorithmische Kompetenz der Menschen investieren.

Ärzte haben den Hippokratischen Eid und Journalisten den Pressekodex. Programmierer brauchen ebenfalls eine Professionsethik. Dabei geht es nicht darum, eine neue Moral für die algorithmische Zeit zu erfinden, sondern vielmehr sicherzustellen, dass unsere analogen Normen und Werte auch in der digitalen Welt gelten. Programmierer und ihre Chefs brauchen Orientierung für die Entwicklung und für den Einsatz der Algorithmen. Nötig sind Prinzipien wie eine klare Kennzeichnung, Nachvollziehbarkeit, Beherrschbarkeit und eindeutige Verantwortlichkeiten.

Die gute Nachricht: In der Branche wächst die Sensibilität für die gesellschaftliche Tragweite ihres Tuns. So protestierten Mitarbeiter von Google, als herauskam, dass sie im Projekt Dragonfly faktisch an einer zensierten Suchmaschine für den chinesischen Markt arbeiteten. Und Studierende von Eliteuniversitäten erklärten, Jobinterviews mit dem US-Konzern abzulehnen, falls er die Arbeit am KI-Projekt Maven für das dortige Verteidigungsministerium fortsetzen sollte. Die Proteste zeigten Erfolge, entsprechende Projekte liefen aus.

Auch aus solchen Gründen arbeiten viele Konzerne derzeit an ihrer Corporate Digital Responsibility. So wie bei der Corporate Social Responsibility formulieren sie eine freiwillige Selbstverpflichtung, an der sie sich im Umgang mit den digitalen Technologien messen lassen müssen. Eine kompetente Öffentlichkeit, die ethisches Verhalten belohnt und unethisches Verhalten sanktioniert, ist dabei zentral. Für Unternehmen kann dann aus einem klaren Bekenntnis zur eigenen Verantwortung durchaus ein Wettbewerbsvorteil entstehen, wie die Märkte für fair produzierte Mode oder fair gehandelte Lebensmittel zeigen. Während die USA oder China kommerzielle und technische Vorreiter in Sachen KI sind, sollte Europa auf soziale und ethische Aspekte algorithmischer Systeme als Alleinstellungsmerkmal setzen. Wenn »Made in Germany« traditionell für zuverlässige Produktqualität steht, könnte KI »Made in Europe« zum Markenzeichen für Verantwortung, für innovative und gesellschaftlich förderliche Technologie werden.

So wichtig wie lesen und schreiben

Noch herrscht in der Bevölkerung große Unkenntnis: Über die Hälfte der Deutschen weiß kaum etwas über Algorithmen. So wie der Buchdruck zur Alphabetisierung führte, muss jetzt mit den Algorithmen eine breite Algorithmic Literacy einhergehen. Unabhängig von Bildungsstand und Beruf sollte jeder in der Lage sein, den Einsatz solcher Systeme zu erkennen, versiert mit ihnen umzugehen und sich im Zweifel gegen fragwürde maschinelle Entscheidung zu wehren. Auskunftsrechte und Beschwerdemöglichkeiten helfen nur dann, wenn die Bevölkerung über genügend Wissen verfügt.

Programmieren wird deshalb nicht zwingend zum Pflichtfach. Auch in der digitalisierten Arbeitswelt bleibt dies ein Job für Spezialisten. Notwendig ist jedoch in der Breite ein Verständnis für fundamentale Mechanismen. Nur wer zumindest grob versteht, welche Konzepte hinter Computerprogrammen liegen und welch unterschiedliche Qualität Daten haben können, kann die Wirkung von Algorithmen bewerten: Nutzen oder schaden sie? Sind sie Teil der Lösung oder Teil des Problems? Diese Fähigkeit wird zur Kulturtechnik, weil Software uns in fast allen Bereichen des Lebens begegnet, bei der Jobsuche, bei der Versicherung, bei Geldanlagen, bei der Internet-Recherche oder auf Dating-Plattformen.

Wer schon als Kind mithilfe einer simplen visuellen Programmiersprache wie Scratch einem Roboter etwas beigebracht hat, begreift besser, dass wir Menschen die Maschinen kontrollieren und nicht umgekehrt. Eine solche Erfahrung lässt Vertrauen und gesunde Skepsis gleichermaßen wachsen. Wer hingegen die Maschinen nur passiv nutzt, dem wird dies nicht gelingen. Algorithmisches Denken ist gewissermaßen die Grammatik der digitalen Gesellschaft: Man braucht sie nicht nur, um eine bestimmte Sprache besser zu sprechen, sondern vor allem, um die Struktur des Gesamtsystems zu verstehen. Großbritannien hat in seiner KI-Strategie als eines der ersten Länder konkrete Schritte beschlossen, um Computational Thinking systematisch in den schulischen Lehrplänen zu verankern und die Informatiklehrer dafür weiterzubilden.

Nur bei der Jugend anzusetzen, genügt allerdings nicht. Algorithmic Literacy erschließt sich für die meisten am besten anhand plakativer Beispiele. Der umstrittene Algorithmus etwa, der den Newsfeed bei Facebook zusammenstellt, ist zwar höchst komplex und streng geheim. Dem Wall Street Journal gelang es trotzdem, seine Funktionsweise zu veranschaulichen. Im amerikanischen Präsidentschaftswahlkampf 2016 stellte die Redaktion zwei Newsfeeds nebeneinander: einen aus typisch republikanischen und einen aus typisch demokratischen Facebook-Foren. So wurde deutlich, wie Facebook seinen Nutzern je nach deren politischer Einstellung zu ein und demselben Vorfall teilweise exakt gegenteilige Interpretationen liefert. Dieser einfache visuelle Vergleich war für die Leser vermutlich erhellender als jedes Theorie-Seminar über Künstliche Intelligenz.

Ähnlich wie die Bundeszentralen für politische Bildung oder für gesundheitliche Aufklärung, die beide mit einem durchaus erzieherischen Auftrag die gesamte Bevölkerung ansprechen, sollte eine neu einzurichtende Bundeszentrale für algorithmische Kompetenz in die Gesellschaft hineinwirken. Sie würde dazu beitragen, dass die öffentliche Debatte jenseits von Verheißungs- oder Horrorszenarien kenntnisreicher geführt wird. Diese derzeitige Polarisierung gilt es zu überwinden, um die Chancen des digitalen Wandels zu nutzen.

Der Staat ist zentraler Akteur dieser gesellschaftlichen Transformation. Die dafür notwendige Kompetenz aufzubauen ist eine seiner größten und drängendsten Aufgaben. Die moderne Verwaltung ist auf algorithmischen Sachverstand angewiesen. Zum einen, um gemeinwohlförderliche Rahmenbedingungen für das Wirken intelligenter Maschinen zu schaffen. Zum anderen, um der eigenen Verantwortung als Betreiber all jener Software gerecht zu werden, die in Polizei-, Finanz- oder Asylbehörden bereits zum Einsatz kommt. Diese Verantwortung ist eine besondere, weil kein Bürger sich den Entscheidungen entziehen kann, die der Staat in Ausübung seines Gewaltmonopols und seiner hoheitlichen Aufgaben trifft.

Wie groß das Interesse, aber auch der Nachholbedarf auf Seiten der Politik ist, zeigte vor wenigen Jahren ein Pilotprogramm zum fachlichen Austausch zwischen Parlamentariern und Digitalexperten in Großbritannien. Das Projekt war durchaus erfolgreich, wenn auch nicht unbedingt so, wie erwartet. Statt die Feinheiten von Blockchain oder Machine Learning auszuleuchten, ging es mehr um digitale Basics: Passwortschutz aktivieren, E-Mails in Ordnern ablegen, Webseiten erneuern. In Deutschland wäre das wohl kaum anders.

Den nötigen Kompetenzaufbau in unserer öffentlichen Verwaltung sollte eine zentrale Agentur für algorithmische Systeme vorantreiben. Kein neues Digitalministerium, sondern eine Institution, die dafür sorgt, dass beim Staat digital überall normal wird. Ihr Auftrag wäre, Expertise zu bündeln, Parlamente, Ministerien, Behörden und bei Bedarf auch Gerichte zu beraten sowie algorithmischen Sachverstand auf- und auszubauen. ▸

Blindes Vertrauen in Software ist gefährlich, denn ihre Entscheidungen bestimmen zunehmend unser Leben. Immer intelligentere Maschinen erfordern immer kompetentere Menschen. Sonst wird die Verheißung einer gerechteren, sichereren, und effizienteren Welt ein Wunschtraum bleiben. Wer gesellschaftlich relevante Algorithmen allein dem freien Spiel des Marktes überlässt, nimmt soziale Kosten in Kauf, die jeden ökonomischen Nutzen bei weitem übersteigen dürften.

Damit die Maschinen den Menschen dienen, ist allerorten mehr Algorithmen-Kompetenz nötig. Die Bevölkerung braucht ein Grundverständnis, um weder Apokalyptikern noch Heilsversprechern auf den Leim zu gehen. Programmierer, Führungskräfte und professionelle Anwender benötigen profundes Wissen und einen ethischen Kompass. Und auch der Staat muss Schritt halten mit der technologischen Entwicklung, um den Tech-Giganten die Stirn bieten zu können. In dieses breite Mehr an Kompetenz müssen wir dringend investieren. Es ist der Schlüssel für echtes Vertrauen. Wir werden es brauchen, damit Mensch und Maschine die komplexen Herausforderungen der Zukunft gemeinsam bewältigen können.

Über die Autoren

Jörg Dräger und Ralph Müller-Eiselt
sind Digitalisierungs- und Bildungsexperten.
Dräger war bis 2008 Hamburger Wissenschaftssenator und ist seitdem Vorstand der Bertelsmann Stiftung.
Müller-Eiselt verantwortet dort das Programm »Megatrends«.
Dieser Beitrag basiert auf ihrem jüngst bei DVA erschienenen Buch **»Wir und die intelligenten Maschinen«**, in dem die Autoren anhand anschaulicher Fallbeispiele die Chancen und Risiken von Algorithmen für jeden von uns beschreiben und konkrete Vorschläge machen, wie wir Künstliche Intelligenz in den Dienst der gesamten Gesellschaft stellen können.

Der Text ist in einer kürzeren Fassung erstmals in der ZEIT vom 11. April 2019 unter dem Titel »Wir Ahnungslosen« erschienen.

Anzeige

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

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

Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.
- exclusives Wording für BvD-Mitglieder (auf Berufsbild DSB zugeschnitten)
- Tätigkeit ‚Auditor für Datenschutz' beitragsfrei eingeschlossen
- niedrige Einsteigerprämie sowie professionelle Beratung

- inkl. DS-GVO
- hohe Deckungssummen zu verbesserten Konditionen

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

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

ALGORITHMENBASIERTE ENTSCHEIDUNGSSYSTEME: VERTRAUEN IST GUT – KONTROLLE IST BESSER

Dr. Miika Blinn, Florian Glatzner

Algorithmenbasierte Entscheidungssysteme, die große Auswirkungen auf die Gesellschaft haben, müssen so gestaltet werden, dass sie für unabhängige Kontrollen zugänglich sind und wichtige Entscheidungen gegenüber betroffenen Verbrauchern transparent werden.

In immer mehr Lebensbereichen werden (selbstlernende) algorithmenbasierte[1] Entscheidungssysteme (Algorithmic Decision Making System, im Folgenden ADM-System) eingesetzt, um automatisiert Entscheidungen über Verbraucherinnen und Verbraucher[2] zu treffen oder vorzubereiten. Es ist davon auszugehen, dass die Anzahl der Lebensbereiche und Anwendungskontexte, in denen diese Systeme eingesetzt werden, weiter zunimmt[3]. Hiervon sind Fragen der Lebensgestaltung, Teilhabemöglichkeiten, Konsumentscheidungen und Autonomie jedes Einzelnen sowie das gesellschaftliche Zusammenleben insgesamt betroffen. Damit verbunden werden grundlegende Fragen aufgeworfen, etwa zu Diskriminierung von Personen und Gruppen oder zu Autonomieverlust und Fremdbestimmung von Verbrauchern (durch beispielsweise Entscheidungsassistenten).

ADM-Systeme können große Auswirkungen auf Individuen und die Gesellschaft haben, stellen aber oft für Außenstehende eine Blackbox dar. Dennoch müssen auch in einer Welt selbstlernender Algorithmen die Einhaltung und Durchsetzung rechtlicher Regelungen sichergestellt sein, um deren Chancen zu nutzen und die Risiken einzudämmen. Solche können etwa hinsichtlich möglicher Diskriminierungen oder Irreführungen von Verbrauchern bestehen.

Unabhängige Kontrolle sicherstellen

Hierfür sollte ein staatlich legitimiertes Kontrollsystem eingerichtet werden, mit dem Ziel, die Risiken von relevanten ADM-Prozessen zu minimieren. Dieses sollte sich durch Vielschichtigkeit auszeichnen und nicht aus einer einzigen Institution bestehen. Es sollte mehrere Elemente (zum Beispiel Betreiberpflichten, Normen und Standards, Aufsichtsbehörden etc.) umfassen, deren Zusammenwirkung eine angemessene Kontrolle sicherstellen kann.

Nicht bei allen ADM-Systemen besteht im gleichen Umfang und in gleicher Tiefe Regulierungsbedarf. Voraussetzung dafür, dass ein ADM-System einer regulatorischen Maßnahme unterworfen wird, sollte sein, dass das ADM-System gesellschaftlich relevante Auswirkungen hat, verbunden mit einem Schadenspotenzial für Individuen und/oder die Gesellschaft. Wird in einem ersten Schritt die Relevanz eines ADM-Systems festgestellt (»Ob«), kann in einem zweiten Schritt die Bestimmung angemessener, fallspezifischer Regulierungsinstrumente (»Wie«) erfolgen (vgl. Abb. 1). Dabei sollte nach dem Ansatz verfahren werden, dass ein steigendes Risikopotenzial mit höheren Eingriffstiefen der regulatorischen Instrumente einhergeht. In diesem Sinne sollten Betreibern relevanter ADM-Prozesse je nach Risiko Verpflichtungen auferlegt werden, wie beispielsweise Transparenzvorgaben, Protokollierungspflichten, ADM-Folgeabschätzung, Audits/Zertifizierungen. Ungeachtet dessen sollten Aufsichtsbehörden als Teil des Kontrollsystems darüber hinaus stets die Befugnis haben, ADM-Systeme vollständig einzusehen und detailliert zu überprüfen (»Inhaltskontrolle«). ▸

[1] Ein Algorithmus ist zunächst eine festgelegte Handlungsanweisung, die auch »analog« festgelegt und ausgeführt werden kann. Vgl. Interview mit Sebastian Stiller in: Algorithmen treffen ins Mark der Macht. in: Politik & Kommunikation (2017), URL: https://www.politik-kommunikation.de/ressorts/artikel/algorithmen-treffen-ins-mark-der-macht-93003943 [Zugriff: 12.04.2019] sowie Zweig, Katharina: Was ist ein Algorithmus? in: AlgorithmWatch, URL: https://algorithmwatch.org/publication/arbeitspapier-was-ist-ein-algorithmus/ [Zugriff: 12.04.2019].
[2] Die gewählte männliche Form bezieht sich immer zugleich auf weibliche und männliche Personen. Wir bitten um Verständnis für den weitgehenden Verzicht auf Doppelbezeichnungen zugunsten einer besseren Lesbarkeit des Textes.
[3] Eine Zusammenstellung von Beispielen für den zunehmenden und vielfältigen Einsatz von ADM-Systemen finden sich in AlgorithmWatch: Atlas der Automatisierung: Automatisierung und Teilhabe in Deutschland (2019), URL: https://atlas.algorithmwatch.org/ [Zugriff: 16.04.2019].

KI & DATENSCHUTZ

Abb. 1: Risikoprüfung und Anwendung von Regulierungsinstrumenten innerhalb des Kontrollsystems

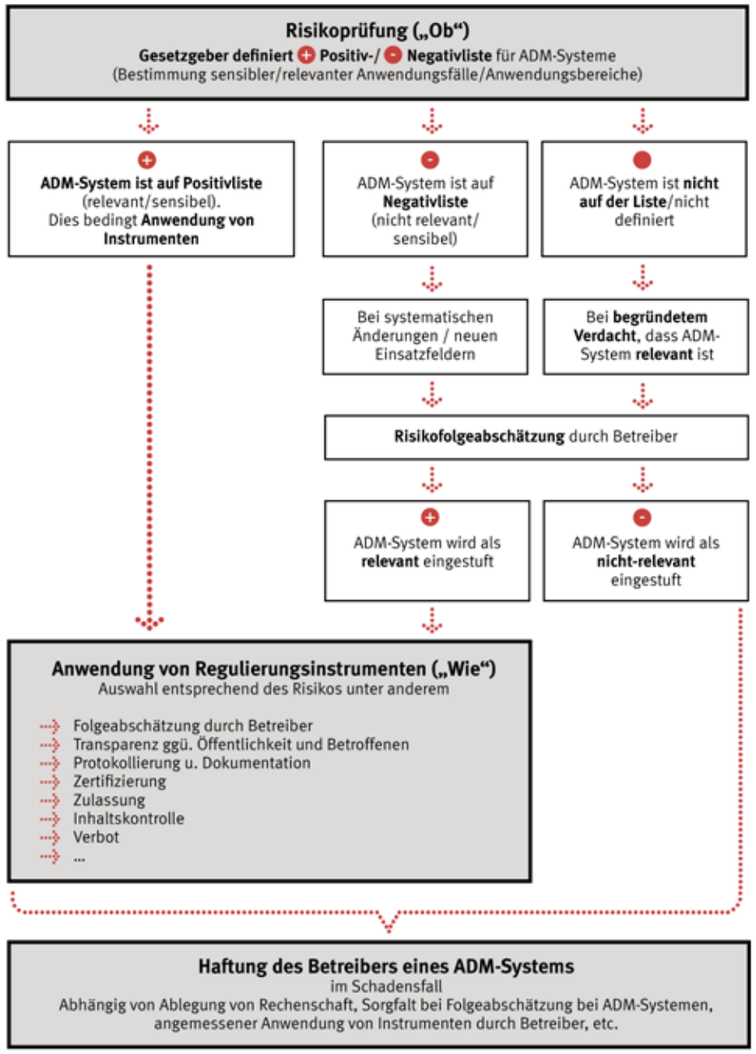
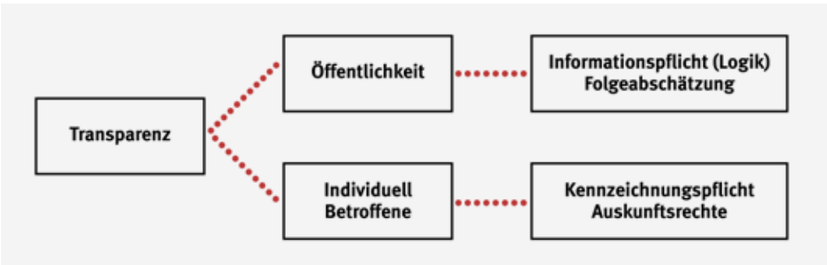


Abb. 2: Übersicht Transparenz gegenüber Öffentlichkeit und Betroffenen



Im Folgenden werden die wichtigsten Elemente, welche für die Etablierung eines effektiven Kontrollsystems erforderlich sind, aufgeführt[4].

1. Risikoprüfung von ADM-Systemen etablieren

Der Gesetzgeber sollte mit Hilfe von Kriterien und einem Prüfschema definieren, welche Anwendungsbereiche oder ADM-Systeme mit einem hohen Schadenspotenzial für Individuen und/oder die Gesellschaft verbunden sein können. Die jeweiligen Anwendungsbereiche/-Fälle sollten einer konkretisierenden, aber nicht abschließenden Positiv- und Negativliste zugeordnet werden.

2. Transparenzen schaffen

Transparenz über den Einsatz und die Arbeitsweise von ADM-Systemen sollte auf zwei Ebenen hergestellt werden (vgl. Abb. 2). Zum einen gegenüber individuell Betroffenen und zum anderen gegenüber der Öffentlichkeit.

Informationspflichten erweitern

Informationspflichten sind eine Grundvoraussetzung, um Transparenz herzustellen und Vertrauen in Systeme zu schaffen, die auf algorithmischen Entscheidungen basieren.

Deshalb sollten Unternehmen stets darüber informieren müssen, wenn ADM-Systeme wichtige Entscheidungen über Verbraucher treffen oder vorbereiten und Angaben über die Konzeption, Reichweite und mögliche Auswirkungen einer solchen Anwendung machen. Nur so können sich die interessierte Öffentlichkeit und potentiell Betroffene ein Bild machen und die ADM-Systeme in Grundzügen bewerten.

Umfassende Risiko Folgeabschätzung für ADM-Systeme einführen

Die Datenschutz-Folgenabschätzung i.S.d. Art. 35 Abs. 1 DSGVO umfasst ausschließlich eine Analyse der Folgen einer Datenverarbeitung auf den Schutz personenbezogener Daten und keine umfassende Risikoanalyse eines ADM-Systems.[5] Bei ADM-Systemen mit einem signifikanten Risikopotenzial ist es aber sachgerecht und zumutbar, dem Betreiber eine umfassende ADM-Folgenabschätzung abzuverlangen.[6] Entsprechende Regelungen bestehen bereits im Gefahrstoffrecht.[7]

Darüber hinaus sollten die Folgenabschätzungen durch die Betreiber veröffentlicht werden müssen. Dies ist Voraussetzung dafür, dass die Öffentlichkeit die grundlegenden Eigenschaften und Risiken von ADM-Systemen (etwa für Vermögen, Eigentum körperliche Integrität und Diskriminierung) einschätzen kann. Dafür muss etwa bekannt sein, auf welcher allgemeinen Datengrundlage ein Machine-Learning-basiertes ADM-System trainiert wurde, welche Datenkategorien einbezogen werden und auf welche Kriterien das System optimiert. Sie sollte neben Informationen zu den zugrundeliegenden Daten und Logik des Modells auch Qualitäts- und Fairnessmaße zu Daten und Modellgüte enthalten, wie etwa zu Bias oder (statistischen) Fehlerquoten[8], die ein System aufweist.

Kennzeichnungspflichten

Zudem sollte bei relevanten ADM-Systemen, die wichtige Entscheidungen über Verbraucher treffen oder vorbereiten, eine Kennzeichnungspflicht eingeführt werden, die Betroffene auf diesen Umstand hinweist. Menschen sollten darauf aufmerksam gemacht werden müssen, wenn sie mit einem ADM-System interagieren (etwa Assistenzsysteme, die Telefonate führen). Diese Transparenz ist Grundvoraussetzung, um Würde und Entscheidungssouveränität von Verbrauchern zu wahren und bewusste Konsumentscheidungen zu ermöglichen. Nur so können sich Verbraucher beispielsweise für oder gegen einen Dienst entscheiden und/oder vor der Inanspruchnahme zusätzliche Informationen einholen und sich gegen Irreführungen wehren.[9]

Auskunftsrechte

Durch die strukturellen Eigenarten von ADM-Systemen besteht das Risiko von Fehlschlüssen der Scheinkausalität, wodurch ein besonderes Schutzbedürfnis ausgelöst wird.[10] Auskunftsrechte sind für Verbraucher zentral, um algorithmenbasierte Entscheidungen nachvollziehen und individuell überprüfen und ggf. anfechten zu können. ▸

[4] Für eine umfassendere Darstellung siehe vzbv: Algorithmenkontrolle, URL: https://www.vzbv.de/pressemitteilung/algorithmen-kontrollieren-geltendes-recht-durchsetzen [Zugriff: 21.06.2019].

[5] Martini, Mario: Grundlinien eines Kontrollsystems für algorithmenbasierte Entscheidungsprozesse. Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes (2018) S. 17-18 »Sonstige Schutzgüter – wie etwa das Vermögen, das Eigentum oder die körperliche Integrität – muss der Verantwortliche demgegenüber nicht zwangsläufig und unmittelbar in seinen Prüfradar integrieren […]. Das Regelungskonzept der DSGVO springt dadurch zu kurz.«

[6] Martini, Mario (2018) (wie Anm. 5), S. 17f., Vgl. ebenso Diakopoulos, Nicholas u. a.: Principles for Accountable Algorithms and a Social Impact Statement for Algorithms, URL: http://www.fatml.org/resources/principles-for-accountable-algorithms [Zugriff: 17.04.2019].

[7] Martini, Mario (2018) (wie Anm. 5). S. 17-18, zur Frage inwieweit es sachgerecht ist, »Diensteanbietern, die grundrechtssensitive oder potenziell gefährdende Algorithmen einsetzen, eine thematisch umfassende Risiko- bzw. Folgenabschätzung abzuverlangen, bevor sie ihre Softwareanwendungen am Markt einsetzen« (S.18) »Die Rechtsordnung kann dem Anbieter einer Softwareanwendung dabei durchaus auch überantworten, bisher unerkannte Gefahren für alle betroffenen Rechtsgüter zu ermitteln; vgl. dazu bspw. die entsprechenden Regelungen im Gefahrstoffrecht: Art. 5 ff. VO (EU) Nr. 1272/2008« (Fn 53, S.18).

[8] So kann es sein, dass ein ADM-System für bestimmte soziale Gruppen höhere Fehlerquoten aufweist als für andere, wodurch diese systematisch benachteiligt werden können. Vgl. Angwin, Julia u. a.: Machine Bias. in: ProPublica (2016), URL: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [Zugriff: 17.04.2019] für den Fall individueller Rückfälligkeitsprognosen. Eine Beschreibung von Fairnessmassen liefern Zweig, Katharina; Krafft, Tobias: Fairness und Qualität algorithmischer Entscheidungen, in: Mohabbat-Kar, Resa/Thapa, Basanta E.P/Parycek, Peter (Hrsg.): (Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, S. 204–227, Berlin, Kompetenzzentrum Öffentliche IT.

[9] Mittlerweile betreffen die meisten Verbraucherbeschwerden bei der U.S. Aufsichtsbehörde für Telekommunikation FCC sogenannte »Robocalls« also Anrufe durch Maschinen, die Verbraucher automatisiert anrufen, teils in betrügerischer Absicht. Federal Communications Commission: Stop Unwanted Robocalls and Texts (2019), URL: https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts [Zugriff: 14.03.2019].

[10] Martini, Mario (2018) (wie Anm. 5) S. 13

KI & DATENSCHUTZ

Wenn eine Entscheidung eines ADM-Systems in grundrechtssensiblen Feldern (zum Beispiel Leib/Leben, Eigentum, Recht auf Schutz personenbezogener Daten) eine rechtliche Wirkung oder eine andere erhebliche Auswirkung auf den Betroffenen zur Folge hat, sollte dieser das Recht erhalten, dass ihm der Verantwortliche das Ergebnis für den Einzelfall erläutern und ihm die zugrundeliegenden Daten, sowie ihre Gewichtung bei der Berechnung konkret in einer nachvollziehbaren Form offenlegen muss.

3. Anwendungsbereich automatisierter Entscheidungen im Einzelfall erweitern

Die Datenschutz-Grundverordnung (DSGVO) regelt insbesondere in Artikel 22 automatisierte Entscheidungen im Einzelfall, soweit personenbezogene Daten verarbeitet werden. Artikel 22 enthält das Recht, grundsätzlich nicht einer solchen Entscheidung unterworfen zu werden. Problematisch ist jedoch, dass die Vorgaben in Artikel 22 DSGVO lediglich Fälle einer vollständig automatisierten Entscheidungsfindung umfasst, die betroffenen Personen gegenüber rechtliche Wirkung entfaltet oder eine andere erhebliche Auswirkung auf sie hat. Dieser enge Anwendungsbereich lässt viele relevante ADM-Systeme unberührt, was zu erheblichen Schutzlücken führt.

Der Anwendungsbereich des Artikel 22 sollte daher auf Entscheidungen ausgedehnt werden, die nicht nur auf einer ausschließlichen, sondern auch auf einer überwiegend automatisierten Verarbeitung von Daten beruhen. Es muss ausgeschlossen werden, dass Unternehmen sich ihrer Verantwortung für ADM-Systeme entziehen, indem sie die entsprechende Entscheidung formal durch einen Menschen vornehmen lassen. Dementsprechend müssen auch die datenschutzrechtlichen Informationspflichten und Auskunftsrechte angepasst werden (siehe oben).

Um außerdem Sicherungsmechanismen einzuziehen und Fehler und Risiken von ADM-Systemen zu reduzieren, sollten rechtliche Vorgaben an diese Systeme dahingehend gemacht werden, dass die zugrundeliegenden und genutzten Daten für die Entscheidungsfindung erheblich sind. Die automatisierte Verarbeitung der Daten muss mit anerkannten mathematisch-statistischen Verfahren erfolgen. Die Prognosetauglichkeit, Validität und Reliabilität des mathematisch-statistischen Verfahrens sollte wissenschaftlich nachgewiesen werden können.

4. Inhaltskontrolle ermöglichen

In besonders sensiblen Anwendungsfeldern sollte die Markteinführung von ADM-Systemen einer ex-ante Kontrolle, also einer Zulassung unterworfen werden. Eine ex-post Kontrolle muss bei relevanten ADM-Systemen durch das Kontrollsystem fortlaufend möglich sein. Die Anwender solcher Systeme sollten verpflichtet sein, kontinuierlich selbst sicherzustellen, dass die von ihnen eingesetzten ADM-Systeme mit dem bestehenden Rechtsrahmen im Einklang stehen. Die von den Anwendern vorgenommenen Prüfungen müssen insbesondere für die zuständige Aufsichtsbehörde überprüfbar und nachvollziehbar sein.

Daher sollte der Einsatz von Kontrollalgorithmen bei der Prüfung der Rechtmäßigkeit von ADM-Systemen rechtlich abgesichert sein, etwa um systematisch nach auffälligen Mustern in Datenbasis und Ergebnissen suchen, die Aufschluss über eine ungerechtfertigte Diskriminierung im Sinne des AGG geben könnten.

Test- und Auditverfahren können dazu dienen, Fehler oder Biases in ADM-Systemen und deren Datengrundlage zu identifizieren. Bei Testergebnissen ist nicht immer eindeutig, ob sie wirklich einen Fehler eines ADM-Systemen aufzeigen, was ihre Beweisfunktion einschränkt.[11] Damit sie ihre Beweisfunktion ausfüllen können, sollte der Gesetzgeber Rahmenbedingungen schaffen, die den Einsatz von technisch-statistischen Tests und Audits rechtlich absichern.

Im Falle eines Rechtsverstoßes sollten die Möglichkeiten der Aufsichtsbehörden von der Anpassung des ADM-Systems bis hin zum Verbot als Ultima Ratio reichen.

5. Nachvollziehbarkeit durch Gestaltung von ADM-Systemen sicherstellen

Verbindliche Standards für die technische Gestaltung und Protokollierung, Dokumentation und Beschreibung von ADM-Systemen sind erforderlich, um diese einer Kontrolle zugänglich zu machen (Nachvollziehbarkeit-by-Design). Betreiber von relevanten ADM-Systemen sollten technische Schnittstellen vorhalten müssen, so dass die zuständigen Aufsichtsbehörden über diese auf das System zugreifen können, um es auf ihre Rechtmäßigkeit sowie technische und methodische Fehler hin überprüfen zu können.

6. Institutionelle Ausgestaltung

Der Gesetzgeber sollte für die zuständigen Aufsichtsbehörden erforderliche Befugnisse (zum Beispiel Auskunfts-, Einsichts- und Zugangsrechte) etablieren, damit diese ADM-Systeme überprüfen und bewerten sowie Rechtsverstöße sanktionieren können. Sollten Schutzlücken identifiziert werden, etwa, weil relevante Anwendungsbereiche von ADM-Systemen keiner direkten Aufsicht unterworfen sind, sollte die Aufsichtslandschaft neu geordnet werden, um diese Schutzlücken zu schließen. Darüber hinaus sollte eine zentrale Unterstützungseinheit etabliert werden, die die weiterhin zuständigen sektorspezifischen Aufsichtsbehörden bei der Kontrolle von ADM-Systemen mit technisch-methodischer Expertise unterstützen kann.

Fazit

Um Vertrauen in die für Außenstehende oft undurchsichtigen ADM-Systeme zu schaffen, bedarf es eines Kontrollsystems, das überprüfen kann, ob algorithmenbasierte Entscheidungssysteme geltendes Recht einhalten und es bei Verstößen durchsetzen. Dafür müssen die Betreiber von gesellschaftlich relevanten ADM-Systemen gegenüber der Öffentlichkeit, Betroffenen und Aufsichtsbehörden Transparenz über den Einsatz und angemessene Nachvollziehbarkeit über Datengrundlage und Logik der Systeme herstellen. Die Nachvollziehbarkeit gegenüber der Aufsicht muss durch Normen und Standards für die Gestaltung der Systeme und Schnittstellen sichergestellt werden.

[11] Beispielsweise hinsichtlich der statistischen Signifikanz. Zum rechtlichen Rahmen von Testverfahren für ADM-Systeme vgl. Gesellschaft für Informatik: Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren. Gutachten der Fachgruppe Rechtsinformatik der Gesellschaft für Informatik e.V. im Auftrag des Sachverständigenrats für Verbraucherfragen, Berlin, URL: www.svr-verbraucherfragen.de/wp-content/uploads/GI_Studie_Algorithmenregulierung.pdf [Zugriff: 07.03.2019]. S. 146ff.

Über die Autoren

Dr. Miika Blinn
Referent im Team Digitales und Medien des Verbraucherzentrale Bundesverbands e.V., Schwerpunkt Algorithmenregulierung

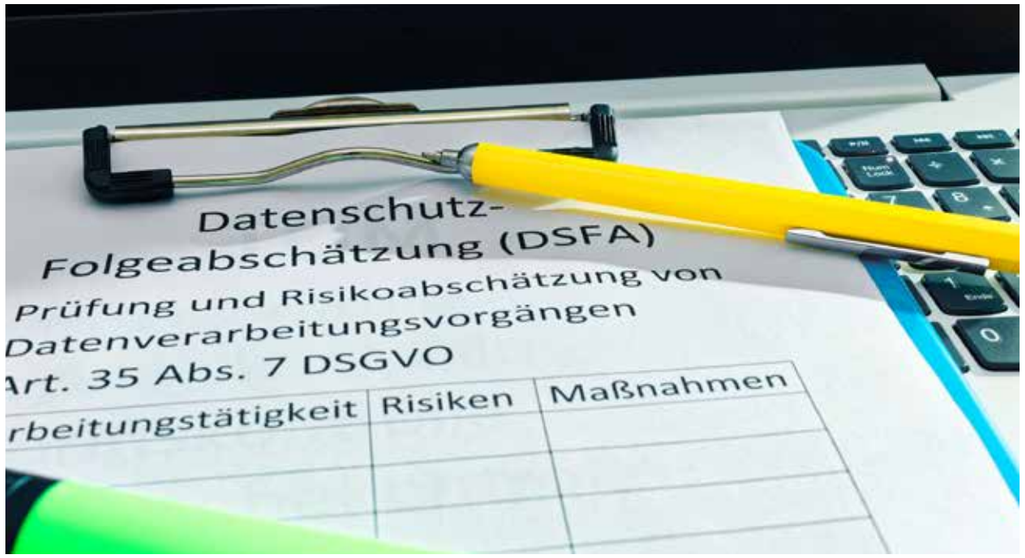
Florian Glatzner
Referent im Team Digitales und Medien des Verbraucherzentrale Bundesverbands e.V., Schwerpunkt Datenschutz

verbraucherzentrale Bundesverband

KI & DATENSCHUTZ

DATENSCHUTZ-FOLGENABSCHÄTZUNG GEMÄSS ISO 29134 IM RAHMEN DER ENTWICKLUNG EINER KI-ANWENDUNG

Beate Beißwenger und Volker Ibisch



I. Einleitung

»Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.« (Art. 35 Datenschutz-Folgenabschätzung, Abs. 1, Satz 1 DSGVO)

Die Datenschutz-Folgenabschätzung (DSFA) ist ein neues Instrument der DSGVO, das mehr ist als nur eine bessere Vorabkontrolle. Denn das Gesetz legt nicht nur fest, wann eine DSFA durchzuführen ist, sondern auch welche verpflichtenden Teile sie enthalten muss. Bei einer Auftragsverarbeitung ist die DSFA vom Verantwortlichen durchzuführen. Der Auftragsverarbeiter hat die Pflicht zu unterstützen.

DATEV hat mittlerweile eine DSFA im Rahmen der Entwicklung einer KI-Anwendung durchgeführt.

Am Beispiel des Projekts »FIBU-Automatisierung« zur (Teil-)Automatisierung der Finanzbuchführung wird auf folgende Aspekte eingegangen:

- Wie stellt man fest, ob für ein neues Produkt bzw. eine neue Anwendung eine Datenschutz-Folgenabschätzung durchzuführen ist?
- Wie ist die Vorgehensweise bei der Planung und Umsetzung einer Datenschutz-Folgenabschätzung gemäß ISO 29134?
- Welche Aufgaben bringt dies mit sich?

Die wesentlichen Bestandteile der DSFA wurden von DATEV vorbereitet, um die Anwender von DATEV FIBU-Automatisierung bei der Durchführung einer ggf. für sie im jeweiligen Nutzungskontext erforderlichen DSFA zu unterstützen.

II. Das Projekt »FIBU-Automatisierung«

Die Mitglieder der DATEV - in diesem Use Case die Steuerberater - arbeiten mit den über ein Mandatsverhältnis verbundenen Unternehmen auf der Cloud-Plattform »DATEV Unternehmen online« zusammen. Auf Basis von elektronisch bereitgestellten Belegen (und weiteren Daten aus Vorsystemen) sollen Buchungssätze unter Einsatz von Methoden der Künstlichen Intelligenz automatisiert erstellt werden.

Im Projekt »FIBU-Automatisierung« entsteht ein System, das noch keine autonome Buchführung ermöglicht. Der Autonomiegrad bewegt sich im Bereich »teilautomatisiert«, d.h. das System ist imstande, in Bezug auf ausgewählte Buchungsvorfälle die zugewiesene Aufgabe selbstständig zu übernehmen und Buchungssätze zu erstellen. Diese Buchungssätze müssen von einem Menschen noch festgeschrieben und damit unveränderbar im Sinne der GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff) gemacht werden.

Das unter anderem aus Data Scientisten bestehende Entwicklungsteam, das die Buchungssatz-Erzeugung und damit den Kern der FIBU-Automatisierung entwickelt, verarbeitet in einer speziell für große Datenmengen ausgelegten IT-Umgebung z.B. die Belegdaten und entwirft und trainiert KI-Modelle. Es erfolgen Auswertungen je Mandanten-Bestand und auch über Mandanten-Bestände mehrerer Kanzleien (DATEV-Mitglieder) hinweg. Zur Verfügung stehen hierbei die Daten aus den Buchführungsbeständen, welche die Kunden für die FIBU-Automatisierung ausgewählt und für die sie jeweils einen Produktvertrag mit der DATEV geschlossen haben.

Von Anfang an in das Projekt eingebunden ist ein juristischer Mitarbeiter des Bereichs Entwicklung, der insbesondere Gesamtprojektleiter und Product Owner (im agilen Entwicklungsprozess für die Eigenschaften des Produkts zuständig) zu allen rechtlichen Themenstellungen berät. Die Beratungsschwerpunkte bilden das IT-Recht und das Datenschutzrecht. Dieser Embedded Lawyer bildet zudem die Schnittstelle zur Abteilung Datenschutz und zur Rechtsabteilung.

Aufgrund seines Beratungsfeldes »mitten im Projekt« ist der Embedded Lawyer prädestiniert für die Aufgaben eines DSFA-Assessors.

III. Ablauf einer Datenschutz-Folgenabschätzung nach ISO/IEC 29134

Eine nach dem methodischen Ansatz nach ISO/IEC 29134 durchgeführte DSFA gliedert sich in folgende Teilbereiche:

- Prüfung der Erforderlichkeit einer DSFA
- Planung: Aufsetzen der DSFA
- Konsultation der interessierten Parteien
- Durchführung der DSFA
- Dokumentation und Veröffentlichung

1. Prüfung der Erforderlichkeit einer Datenschutz-Folgenabschätzung

Zunächst – und das ist eines der wichtigsten Arbeitspakete – ist zu analysieren, welche Verarbeitungsvorgänge beim Einsatz der Anwendung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben.

Anhand eines Schaubildes, das - für alle Domänen (Techniker, Juristen usw.) verständlich - die beteiligten Systeme und Datenverarbeitungsabläufe visualisiert, wird der Anwendungsbereich der DSFA definiert. Für die DATEV FIBU-Automatisierung ergab sich, dass dies die Verarbeitungsvorgänge zur Erstellung der Buchungssätze im DATEV-RZ sind.

Im Zuge der Wesentlichkeitsprüfung gemäß der Leitlinien zur Datenschutz-Folgenabschätzung WP 248 Rev. 01 der Datenschutzgruppe nach Artikel 29 waren sich Fachbereich und Abteilung Datenschutz einig, dass es Kunden (Auftraggeber) geben kann, die für die DATEV-FIBU-Automatisierung eine DSFA gemäß Art. 35 DSGVO durchführen wollen. ▸

KI & DATENSCHUTZ

Das Produkt »DATEV FIBU-Automatisierung« kann bei der Verarbeitung von berufsrechtlich geschützten Daten (auch besondere Kategorien personenbezogener Daten) in großem Umfang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben.

Somit können – je nach Kunden-Szenario – folgende Wesentlichkeitskriterien einschlägig sein:

- Umfängliche Verarbeitung von berufsrechtlich geschützten Daten
- Sensible Daten
- Kombinierte Datenbestände (z.B. von mehr als einem Mandanten)
- Hinderung Betroffener an der Ausübung von Rechten

Das DSFA-Team sah das Wesentlichkeitskriterium »Innovative Verarbeitungen« ebenso wie den Blacklist-Fall »Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person« als nicht gegeben. Dies wirkte sich aber auf die Feststellung der ausreichenden Anzahl von erfüllten Wesentlichkeitskriterien nicht aus.

2. Planung: Aufsetzen der DSFA

a. Projektorganisation

Die Vorbereitung erfolgte in einem eigenen Projekt unter der Leitung eines DSFA-Assessors mit Projektteam aus Entwicklung, Produktion, Informationssicherheit, Rechtsabteilung und Kundenkommunikation. Datenschutzrechtliche Beratung erfolgte durch die Abteilung Datenschutz und den Bereichsbeauftragten für den Datenschutz in der Entwicklung.

Ein DSFA-Assessor sollte über folgende Skills verfügen:

- Mitarbeiter(in) mit Produktkenntnissen
- Datenschutzrechtliches Basiswissen
- Risikomanagement Basiswissen
- Technisches Grundverständnis
- Projektmanagement
- Moderation (von Workshops)
- Erstellung umfangreicher Berichte

Auf Basis des Ergebnisses der Erforderlichkeitsprüfung wurde vom Management zur Durchführung der DSFA ein Mandat vergeben. Die Dokumentation inkl. Projektplan, Aufwandsschätzung und Budgetierung erfolgte in einem Projekt-SharePoint; für das Management-Reporting wurden die Daten in einem Business Model Canvas-Steckbrief bzw. -Status aggregiert.

b. Beschreibung des Untersuchungsgegenstandes

Der neben der »Konsultation der interessierten Parteien« aufwandsintensivste Arbeitsschritt ist die Beschreibung des **Untersuchungsgegenstandes** mit:

- Systemanforderungen
- Systemdesign
- Betriebliche Pläne und Verfahren/Abläufe
- Angewendete Risikokriterien

Einen Schwerpunkt der Systemanforderungen bildet die Darstellung der **Rechtsgrundlagen und Zwecke** für die Verarbeitung – Angaben, die auch für das Verarbeitungsverzeichnis benötigt werden.

Im Projekt FIBU-Automatisierung reduzierte die Möglichkeit, auf die bestehende DP42-Datenschutz-Dokumentation (DATEV-interner Standard) zurückgreifen zu können, die Aufwände deutlich.

Exkurs:
Bei der DP42-Dokumentation handelt es sich um einen bei DATEV entwickelten internen Standard zur Dokumentation aller datenschutzrechtlichen Aspekte eines IT-Systems (Produkt, Anwendung):

- Informationen für das Verarbeitungsverzeichnis
- Input für Leistungsbeschreibung und Datenschutz-Steckbrief
- Legitimationstatbestände
- Löschkonzept
- Dokumentation von Abstimmergebnissen mit Stakeholdern

Die **Systembeschreibung** erfolgte in Form der Beschreibung der Systemarchitektur und der Datenflüsse.

Nachdem die Software bei DATEV erstellt wird, sind tiefergehende Dokumentationen vorhanden, u.a. eine Softwarearchitektur-Dokumentation. Teile konnten daraus übernommen werden, jedoch mussten zur besseren Verständlichkeit für die Zielgruppe Beschreibungen abstrahiert bzw. mit weiteren Informationen versehen werden.

Die **Darstellung des Informationsflusses** erfolgte durch Zusammenführung von Daten aus verschiedenen Dokumentationen durch den DSFA-Assessor. Sie umfasst Informationen zu den Themen:

- Datenerhebung
- Zweck
- Verantwortlichkeiten
- Vertragsbeziehungen
- Datenübermittlungen an Dritte
- Datenverarbeitung
- Datenlöschung
- Informationssicherheitskonzept

3. Konsultation der interessierten Parteien

Nachdem eine Vielzahl von Personen von den Datenverarbeitungen beim Einsatz von DATEV FIBU-Automatisierung betroffen sind, wurde deren Standpunkt durch eine gemäß Art. 35 Abs. 9 DSGVO optional durchzuführende **externe Konsultation** eingeholt.

Als Vertreter der Mandanten von Mitgliedern der DATEV und deren Geschäftspartner wurden mit einem Vertreter der IHK im Rahmen zweier Termine in Nürnberg die aus seiner Sicht bestehenden Datenschutzrisiken identifiziert und die Berücksichtigung seiner Hinweise in der DSFA besprochen.

Als Vertreter der Auftraggeber/Mitglieder der DATEV wurde im Zuge dessen ein Steuerberater beigeladen.

Im **ersten Termin** wurde den Teilnehmern – nach einer Einführung in das Thema »Datenschutz-Folgenabschätzung« – das Produkt »DATEV FIBU-Automatisierung«, der zu untersuchende Geschäftsprozess und der Anwendungsbereich der Datenschutz-Folgenabschätzung durch den in diesem Kontext zuständigen Product Owner vorgestellt. Nach einer Hinführung zum Thema »Identifikation von Datenschutz-Risiken«, u.a. Erläuterung der Datenschutz-Prinzipien, erarbeiteten die Vertreter der interessierten Parteien die aus ihrer Sicht beim Einsatz von DATEV FIBU-Automatisierung je Datenschutz-Prinzip bestehenden Datenschutz-Risiken. Es kamen auch »good implementations« zur Sprache.

Im **zweiten Termin** wurde zu den identifizierten Risiken die Bewertung durch das DATEV-DSFA-Team vorgestellt. Die Berichte zur DSFA (On Demand-Bericht, öffentlicher Bericht) wurden von den Teilnehmern auf angemessene Berücksichtigung ihrer Ansprüche und Darstellung ihrer Belange geprüft und die Inhalte mit dem DSFA-Team abgestimmt.

Zusätzlich wurden Datenschutzrisiken für die relevanten Anspruchsgruppen im Rahmen mehrerer Workshops mit Mitgliedern des DSFA-Projektteams identifiziert **(interne Beteiligung interessierter Parteien)**. Auch hier erfolgten zunächst eine Einführung in das Thema »Datenschutz-Folgenabschätzung« und eine Erläuterung der Datenschutz-Prinzipien.

Die im Rahmen der internen und externen Konsultationen gewonnenen Erkenntnisse waren Grundlage für die **Risikoanalyse und Risikobewertung** des DATEV-DSFA-Assessors mit Vertretern der Abteilung Datenschutz und dem Bereichsbeauftragten für den Datenschutz in der Entwicklung. Der Bereichsbeauftragte für den Datenschutz hat die Aufgabe eines Datenschutz-Koordinators.

4. Durchführung der DSFA

a. Festlegung der Risikoquellen

Zur Festlegung der Risikoquellen konnte auf das Erfahrungswissen von IT-Sicherheitsrisikoanalysen nach ISO 27001 zurückgegriffen werden. Betrachtet wurden nur spezifische Risiken für die DATEV FIBU-Automatisierung. Als Risikoquellen erkannte das DSFA-Kernteam die in unterschiedlichen Rollen mit der Verarbeitung der Daten betrauten DATEV-Mitarbeiter ▸

(Data-Scientist, Administratoren…), die mit der Auswahl der Daten in den Kanzleien betrauten Personen (Mitarbeiter und Management), unberechtigte Zugriffe durch Mitarbeiter staatlicher Stellen sowie technische Probleme durch Hard- oder Software.

b. Identifikation von Datenschutzrisiken
Um die Risiken für die Rechte und Freiheiten der Betroffenen möglichst umfassend zu erkennen, wurden mehrere Workshops mit den internen Beteiligten sowie eine Konsultation der externen interessierten Parteien durchgeführt. Dieses Vorgehen erwies sich als zielführend, da durch die Beteiligung der Kollegen mit technischer Expertise eine umfassende Betrachtung der technischen Risiken erfolgte. Durch die Beteiligung der externen interessierten Parteien wurde die Risikobetrachtung noch um die Risiken, die beim Auftraggeber entstehen können und die »Ängste der Betroffenen« ergänzt.

c. Analyse und Bewertung der Datenschutzrisiken
Nachdem die Risiken zusammen mit allen interessierten Parteien beschrieben waren, wurden sie durch das DSFA-Kernteam einzeln analysiert und bewertet. Auch hier wurden die bekannten Mechanismen der IT-Sicherheitsrisikoanalyse angewandt. Das Risiko »Missbrauch der Daten durch die Data Scientisten« ergab den höchsten Risikowert. Nach der Bewertung der dagegen getroffenen Maßnahmen u.a. spezielle Zugänge, Protokollierung und Auditierung der Tätigkeit sowie weitere organisatorische Maßnahmen, verblieb kein hohes Risiko. Auch die Bewertung der anderen Risiken ergab kein hohes Risiko, sodass eine Konsultation der Aufsichtsbehörde nicht erforderlich war.

5. Dokumentation und Veröffentlichung der Berichte

Die letzte Phase einer Datenschutz-Folgenabschätzung umfasst gemäß Kapitel 6.5 der ISO/IEC 29134 folgende Arbeitspakete:

- Bericht(e) erstellen
- Berichte veröffentlichen
- Risikobehandlungsmaßnahmenplan umsetzen
- DSFA überprüfen und auditieren
- Regelmäßige Überprüfung der DSFA

Eine zentrale Aufgabe des DSFA-Assessors ist die nachhaltige projektbegleitende Dokumentation der Datenschutz-Folgenabschätzung. Es empfiehlt sich, diese in einem internen Bericht, der Informationen (inkl. Verweise auf weiterführende Dokumente wie z.B. Protokolle von Workshops und Konsultationsterminen) zu allen Teilbereichen der DSFA enthält, zusammenzufassen.

Aus diesem Bericht, der auch Geschäftsgeheimnisse enthalten kann und somit allenfalls im Rahmen von Konsultationen mit Aufsichtsbehörden zum Einsatz kommt, kann die sog. »Public Summary«, der öffentliche Bericht, extrahiert werden. Im Kontext FIBU-Automatisierung wird die Veröffentlichung in der öffentlich zugänglichen DATEV-Informations-Datenbank erfolgen.

Im Bedarfsfall erhalten Anwender von DATEV FIBU-Automatisierung auf Anfrage einen umfangreicheren sog. »On Demand-Bericht«, der sie bei der Durchführung einer ggf. für sie im jeweiligen Nutzungskontext erforderlichen Datenschutz-Folgenabschätzung unterstützt.

Die Cloud-Anwendung DATEV FIBU-Automatisierung hat kein hohes Datenschutzrisiko zur Folge. Die bereits wirksam umgesetzten und regelmäßig überprüften Risikobehandlungsmaßnahmen der DATEV sind angemessen, um ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen ausschließen zu können.

Die Angemessenheit der Durchführung der DSFA wurde – wie von ISO/IEC 29134 empfohlen – durch einen unabhängigen Auditor verifiziert.

Auch wenn die DSFA mit Veröffentlichung des Berichts abgeschlossen scheint, begleitet dieses neue Instrument der DSGVO eine Anwendung während ihres gesamten Lebenszyklus. Die DSFA ist regelmäßig spätestens nach Ablauf von 3 Jahren zu überprüfen. Dies stellt eine der vielfältigen Aufgaben eines Product Owners dar.

IV. Die Aufgaben im Überblick

Prüfung der Erforderlichkeit einer DSFA

Anhand der Blacklist der deutschen Aufsichtsbehörden und der Wesentlichkeitskriterien der Art 29 Gruppe überprüfen, ob von einer Verarbeitung hohe Risiken für die Rechte und Freiheiten natürlicher Personen ausgehen. Wenn ja, ist eine DSFA durchzuführen.

Aufsetzen der DSFA

Welche Verarbeitungsvorgänge verursachen diese Risiken, was ist im Rahmen der DSFA zu betrachten? Wer sind die interessierten Parteien?

Wer ist bei der DSFA innerhalb und außerhalb des Unternehmens einzubeziehen?

Konsultation der interessierten Parteien

In ersten Schritt dient die Konsultation der interessierten Parteien der Identifikation der Risiken; aber auch einer Bewertung der getroffenen Maßnahmen.

Durchführung der DSFA

Obwohl die DSFA in Form einer klassischen Risikoanalyse erfolgt, stehen nicht die Risiken für das Unternehmen, sondern die Risiken für die Rechte und Freiheiten der betroffenen Personen im Fokus.

V. Zusammenfassung

Die ISO/IEC 29134 ist ein geeignetes Vorgehen zur Durchführung einer DSFA.

Den nicht geringen Aufwand einer DSFA bereits vorab adäquat einzuschätzen, ist äußerst empfehlenswert. Sind neue IT-Systeme in Planung, für die eine DSFA erforderlich ist, sollte diese bereits entwicklungsbegleitend erfolgen.

Über die Autoren

Beate Beißwenger
arbeitet als Datenschutz-Referentin für den Datenschutzbeauftragten der DATEV eG.

Volker Ibisch, LL.M. (Legal Informatics)
ist Rechtsanwalt bei der DATEV eG und berät als Embedded Lawyer Entwicklungsprojekte in allen Fragen zu Recht und Datenschutz. Er leitete als DSFA-Assessor die Datenschutz-Folgenabschätzung im Projekt FIBU-Automatisierung.

Zum Unternehmen:
DATEV steht für »Datenverarbeitung« und ist eine aus mehr als 40.000 Mitgliedern bestehende Genossenschaft für steuerberatende Berufe. Das Leistungsspektrum von DATEV umfasst Software für Rechnungswesen, Personalwirtschaft, betriebswirtschaftliche Beratung, Steuerberechnung und Organisation von Unternehmen und Kanzleien.

▶ www.datev.de

Anzeige

www.bvdnet.de

BvD e.V.
DATENSCHUTZ GESTALTEN

Datenschutz betrifft uns alle
30 Jahre BvD

Gemeinsam für einen starken Datenschutz:

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert seit 30 Jahren die beruflichen Interessen der Datenschutzbeauftragten in Behörden und Betrieben und setzt sich aktiv für die weitere Akzeptanz des Berufsbildes „Datenschutzbeauftragter" ein – als einziger Verband in Deutschland.

Der BvD in Zahlen:

- gegründet 1989
- Mitglieder: 1.600
- Firmenmitglieder: 722
- bundesweit 11 Regionalgruppen und 9 Arbeitskreise zu Fachthemen

(Stand: Januar 2019)

BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) E. V. | BUDAPESTER STRASSE 31, 10787 BERLIN
TELEFON: (030) 26 36 77 60 | TELEFAX: (030) 26 36 77 63 | E-MAIL: BVD-GS@BVDNET.DE | INTERNET: WWW.BVDNET.DE

KI IM ANWENDUNGSFELD DER FRAUD PREVENTION

Prof. Dr. Oliver Weissmann und Mirjam H. Steinfeld, Mag iur.

Im folgenden Artikel soll erläutert werden, ob und wie sich künstliche Intelligenz (KI) als Lösung (II.) zur Erfüllung der Verpflichtungen nach dem Geldwäschegesetz (GWG) (I.) anbietet und wie dies unter Beachtung der datenschutzrechtlichen Vorgaben (III.) möglich sein könnte.

I. Was ist Geldwäscheprävention (Anti-Money-Laundering/AML)?

Wer glaubt, sich über einen Neukunden einfach nur freuen zu können, wird kontinuierlich (insb. durch wachsende EU-Regulierung) eines Besseren belehrt: Nicht nur Finanzinstitute und Versicherungen müssen inzwischen prüfen, mit wem sie sich vertraglich binden (Know-Your-Customer/KYC). Insbesondere nach der letzten (fünften) Geldwäsche-Richtlinie (vom 30.05.2018) kann (beinahe) jeder Unternehmer zu dem Kreis der »Verpflichteten« gehören.

Was also ist Geldwäsche, wie wird dieser vorgebeugt und wer ist von welchen Verpflichtungen betroffen?

Zunächst ist festzuhalten, dass Geldwäsche überall dort stattfindet, wo Einnahmen aus illegalen Geschäften in den legalen Finanzkreislauf eingeführt werden, unter Verschleierung ihres eigentlichen Ursprungs (vgl. § 261 StGB). Da hierdurch erhebliche Nachteile für alle ehrlichen Marktteilnehmer entstehen und dem Problem nur durch internationale Kooperation begegnet werden kann, wurden in den vergangenen 30 Jahren diverse Gesetzgebungsvorhaben auf den Weg gebracht[1]. Ursprünglich wurden nur Finanzunternehmen (Banken und Versicherungen) angesprochen (verpflichtet), bestimmte Maßnahmen zu ergreifen, um sicherzustellen, dass ihre Institutionen nicht zum Zweck der Geldwäsche missbraucht werden.

Seitdem ist der Kreis der Verpflichteten deutlich erweitert worden (vgl. § 2 GWG). So gehören inzwischen auch die »Güterhändler« (§ 2 Abs. 1 Nr. 16 GWG), wobei hierunter »jede Person, die gewerblich Güter veräußert« zu verstehen ist (§ 1 Abs. 9 GWG), ebenfalls zu den Verpflichteten, sofern sie Bargeld in Höhe von 10.000 EUR annehmen oder selbst zahlen.

All diese Verpflichteten haben für ein angemessenes Risikomanagementsystem (vgl. § 4 GWG) zu sorgen, durch welches u.a. sichergestellt wird, dass die Geschäftspartner identifiziert und ihre »wirtschaftlich Berechtigten« (§ 11 GWG) offengelegt werden und ob es sich bei diesen Personen um eine politisch exponierte Person handelt (PEP). Dabei muss ein System bestehen, welches die Geschäftsbeziehung kontinuierlich überwacht, um im Falle eines Verdachts auf Geldwäsche eine entsprechende Meldung (§ 43 GWG) abgeben zu können.

Daraus folgt, dass diverse Unternehmen (als Verpflichtete) vor der Herausforderung stehen, hochkomplexe Vorgänge innerhalb ihres Unternehmens »live« zu überwachen, wenn sie sich nicht selbst eines Bußgeldes in erheblicher Höhe (§ 56 Abs. 2 GWG) ausgesetzt sehen wollen.

II. Was hat das alles mit KI zu tun?

Wie kann bzw. soll nun also diese Aufgabe wahrgenommen werden, ohne dass der gesamte Betrieb »lahmgelegt« oder aber ein erheblicher personeller und kostenintensiver Aufwand betrieben wird? Aktuell wird der Einsatz von KI in einer Vielzahl von Bereichen erprobt und in einer noch größeren Vielzahl von möglichen Einsatzgebieten diskutiert. Hierzu gehört auch der umfangreiche Bereich der Fraud Prevention.

Grundsätzlich ist unter KI das Bestreben zu verstehen, Maschinen dahingehend zu bauen bzw. Programme dahingehend zu programmieren, dass diese sich – ähnlich der menschlichen Intelligenz – verhalten bzw. denken. Dabei wird

[1] Steinfeld, Recht innovativ 01/2019, 34 (34).

zwischen einer starken und einer schwachen KI unterschieden. Letzere ist in der Lage, in komplexen ungeordeneten Daten Strukturen zu finden. Detaillierte Definitionen zu KI existieren zwar, jedoch hat sich hier bislang keine als herrschend durchgesetzt.[2]

Grundlage von KI sind Algorithmen. »Einfache« Algorithmen basieren auf dem Prinzip der wenn-dann-Logik (wenn »0« dann »aus«), ein Verhalten muss also präzise beschreibbar sein, um es zu verarbeiten. KI soll diese Logik weit hinter sich lassen, indem die Algorithmen »trainiert« werden, d.h. Muster werden in den unstrukturierten Daten ermittelt und es werden entsprechende Klassen gebildet. So müsste im hier diskutierten Fall der Algorithmus mit Trainingsdaten gefüttert werden, bei denen »normale« Transaktionen aufgezeigt werden, die als »unbedenklich« und sodann »auffällige« Transaktionen, die als »risikobehaftet« deklariert werden.

Hierbei zeigt sich auch sogleich eine der ersten großen Herausforderungen der KI: Sie ist nicht von Anfang an intelligent, sondern sie wird es erst durch Lernen. Dies bedeutet, dass selbst der beste Algorithmus angelernt und folglich mit reichlich Trainingsdaten angefüttert werden muss (die erforderliche Anzahl von Datensätzen kann hier durchaus in die Millionen gehen).[3] Hat die KI genug Trainingsdaten zum Lernen, so entfernt sie sich zunehmend von dem einfachen (wenn-dann-)Algorithmus. Die KI ist jetzt nämlich in der Lage, eigene Muster, Verbindungen und Zusammenhänge zu erkennen, die weit über diese einfache Logik hinausgehen. Problematisch hieran ist jedoch, dass dadurch das Ergebnis nur noch beschränkt nachvollziehbar ist, da der Vorgang der KI mit einer »black box« zu vergleichen ist: Auf der einen Seite wird die Aufgaben-/Fragestellung eingegeben, auf der anderen Seite kommt das Ergebnis raus. Die »gedankliche« Leistung dazwischen tritt nicht nach außen. Übertragen auf die zwei Klassen »normale« und »auffällige« Transaktion sind die Entscheidungen des Kategorierers nicht trivial nachvollziehbar. Sie liegt in dem aus Trainingsdaten konditionierten Netz, welches sich zudem kontinuierlich weiter entwickeln kann.

Hieran schließt sich auch nahtlos die nächste Frage an: Wenn keiner weiß, wie aus der Ausgangslage eine Entscheidung der KI wurde, wer ist dann hierfür verantwortlich?[4] Wer wäre (in unserem Fall) dafür verantwortlich, wenn beispielsweise eine Überweisung (grundlos) angehalten wird und damit dem Überweisenden ein Schaden entsteht? Diese Frage zu beantworten würde zweifelsohne den Rahmen dieses Artikels sprengen. Gleichzeitig ist diese Frage von großer Erheblichkeit bei der Einrichtung eines KI-basierten AML-Systems, insbesondere unter Beachtung der datenschutzrechtlichen Anforderungen.

III. Und wie vereint man dies mit dem Datenschutz?

Die Erfüllung der Pflichten nach dem GWG bezieht sich zu einem erheblichen Teil auf die Verarbeitung von personenbezogenen Daten, weshalb die DSGVO und das BDSG grundsätzlich einschlägig sind. Die Rechtsgrundlage für die Verarbeitung ist schnell gefunden, lässt sie sich doch ▸

[2] Pieper, BvD-News 01/2019, 14 (14)

[3] https://www.heise.de/newsticker/meldung/Datenforscherin-Kuenstliche-Intelligenz-ist-kaputt-4447500.html zuletzt besucht am 21.06.2019

[4] Otto, Recht innovativ 02/2018, 68 (68)

DATENSCHUTZPRAXIS

eindeutig aus Art. 6 Abs. 1 lit. c) DSGVO i.V.m. dem GWG begründen. Damit wäre zwar die grundsätzliche Zulässigkeit der Datenverarbeitung begründet, jedoch ist davon noch nicht das »Wie« erfasst.

Dieser Art der Verarbeitung könnte Art. 22 Abs. 1 DSGVO entgegenstehen, wonach jeder Betroffene das Recht auf eine »menschliche« – mithin nicht vollautomatisierte - Entscheidung hat. Diese Einschränkung trifft vorliegend allerdings nicht zu, da zum einen der europäische Gesetzgeber in Art. 22 Abs. 2 DSGVO eine Ausnahme zugunsten gesetzlicher Verpflichtungen geschaffen hat und zum anderen laut Erwägungsgrund 71 (zur DSGVO) es die Absicht des Gesetzgebers war, dass Art. 22 DSGVO auf Verfahren zur Überwachung von Betrug und Steuerhinterziehung nicht anwendbar ist. Dies geschah wohl vor dem Hintergrund, dass sich dem Gesetzgeber aufdrängte, dass die Erfüllung der Vielzahl von Verpflichtungen im laufenden Geschäftsbetrieb ohne automatisierte Entscheidungen schlichtweg nicht möglich ist.

Von diesen Überlegungen abgesehen stellt sich aber auch die Frage, ob es sich bei einem entsprechenden KI-basierten AML-System überhaupt um eine automatisierte Entscheidung handelt. Von Art. 22 DSGVO werden Verfahren nämlich nicht erfasst, die lediglich der Entscheidungsvorbereitung dienen. Vorbereitend kann allerdings nur ein solches Verfahren sein, bei dem der Schwerpunkt der Entscheidung beim Menschen verbleibt und dieser nicht nur lediglich »einen Knopf drückt«[5]. Ein AML-System, welches aus der Masse der Transaktionen einer organisatorisch zuständigen Stelle Verdachtsfälle präsentiert, ohne dass sich hieraus eine direkte/zwangsläufige Konsequenz ergibt, wird wohl ohnehin nur als vorbereitend und somit nicht als eine nicht dem Art. 22 DSGVO unterfallende Verarbeitung zu werten sein. Sofern jedoch eine direkte »Außenwirkung« von dieser Entscheidung ausgeht (bspw. Einfrieren einer Überweisung), so wäre diese – wenn auch nicht endgültig – möglicherweise als vollautomatisiert zu betrachten.

Ob nun vollautomatisiert oder nicht, so wird aus der Nutzung eines entsprechenden AML-Systems jedenfalls die Pflicht zur Vornahme einer Datenschutzfolgenabschätzung (DSFA) gem. Art. 35 Abs. 1 DSGVO (neue Technologie) oder Art. 35 Abs. 3 lit. a) DSGVO (automatisierte Verarbeitung als Grundlage von Entscheidungen) folgen. Bei der nach Art. 35 Abs. 7 DSGVO vorzunehmenden Abwägung dürften sich jedoch grundsätzlich keine größeren Schwierigkeiten auftun, da der Bekämpfung von Geldwäsche und der Funktionalität des Marktes wohl größeres Gewicht als dem Interesse des Betroffenen an einer Einzelfallentscheidung zuzumessen wäre.

Schwieriger stellt sich da die Wahrung der Betroffenenrechte, insbesondere nach Art. 12 DSGVO, dar. Hiernach müssen Betroffene transparent und in klarer und verständlicher Weise über die Verarbeitung ihrer personenbezogenen Daten informiert werden. Wie soll nun aber der Verantwortliche den Betroffenen über eine Verarbeitung informieren, von der er selbst nicht weiß, wie sie geschieht (»black box«)? Letztendlich wird es wohl darauf ankommen, dem Betroffenen in groben Zügen das grundsätzliche Verfahren mit den einschlägigen Parametern zu erläutern. Hierfür könnte gegebenenfalls das sog. LIME-Verfahren (Local Interpretable Model-Agnostic Explanations) herangezogen werden, welches zwar keine exakten Maßstäbe, dafür jedoch wenigstens Näherungswerte liefert.

Alternativ, für den Fall des nicht vollautomatisierten Verfahrens, wäre es auch möglich dem Betroffenen mitzuteilen, dass seine Daten im Rahmen einer vorbereitenden Maßnahme durch einen Algorithmus vorverarbeitet werden. Die algorithmische Einteilung in Klassen ist nun wirklich nichts Neues (siehe SCHUFA). Der einzige Unterschied ist, dass die Zuordnung früher algorithmisch exakt beschrieben werden konnte. Dennoch bekamen Betroffene vormals auch keinen uneingeschränkten Einblick in die Algorithmen (denn diese waren z.T. gut gehütete Geschäftsgeheimnisse[6]), sondern bekamen die Information, dass sie klassifiziert wurden. Es geht also in der Frage vielmehr um das »Wie« als um das »Ob«. Entscheidend wird daher vielmehr sein, dass sichergestellt wird, dass am Ende jeder Fall durch eine sachkundige Person entschieden wird.

Selbst unter Beachtung all dieser datenschutzrechtlichen Vorgaben bleibt die grundsätzliche Problematik der Pflichten nach dem GWG unberührt: Es werden immer mehr Daten von immer mehr Stellen/Verarbeitern gesammelt zu dem einzigen Zweck diese – über nationale Grenzen hinweg – zusammenzuführen und auszutauschen. So hilft auch das strengste Datenschutzgesetz nicht, wenn es der Gesetzgeber ist, der stets neue Rechtsgrundlagen zur Durchbrechung des Prinzips der Datensparsamkeit schafft und sich vielmehr selbst als der größte Datensammler entpuppt[7].

IV. Fazit:

Die DSGVO ist grundsätzlich Technologie-neutral und somit stets entsprechend auf die aktuellen Entwicklungen auszulegen. Dementsprechend ist es, wie oben aufgezeigt, durchaus möglich KI datenschutzkonform zur Erfüllung von gesetzlichen »Compliance-Pflichten« einzusetzen. Ausschlaggebend für die Datenschutzkonformität wird daher vor allen Dingen die Einteilung in vorbereitende und vollautomatisierte Verfahren sowie die Wahrung der Informationspflichten sein.

[5] Hoeren/Niehoff, Rechtswissenschaft 2018, 47 (53)

[6] BGH 28.01.2014 »SCHUFA-Urteil«, BGHZ 200, 38

[7] Es sei daher an dieser Stelle nur ein kurzer Ausblick auf die bereits verabschiedete Richtlinie zu »meldepflichtigen grenzüberschreitende Steuergestaltungen« (RL (EU) 2018/822) verwiesen. Doch dies ist ein weiteres ganz eigenes Datenschutzproblem.

Über die Autoren

Rechtsanwältin Mirjam Hannah Steinfeld, Mag. iur.
Fachanwältin für Strafrecht
führt seit 2012 ihre auf Strafrecht spezialisierte Kanzlei und ist zudem Mitinhaberin der Schmidt Steinfeld Solutions, die u.a. im Bereich Compliance berät. Sie ist außerdem im Herausgeberbeirat der Fachzeitschrift „Recht innovativ“ und als Lehrbeauftragte für Strafrecht an der Hochschule Rhein-Main tätig. Seit Oktober 2018 belegt sie zudem den Studiengang MBA in „Wirtschaftskriminalität und Compliance“ an der Steinbeis-Hochschule.

Prof. Dr. Oliver Weissmann
ist Inhaber der xiv-consult GmbH. Für die ISO betreut er seit 1998 unterschiedliche Standards als Editor und Projektverantwortlicher (bspw. ISO/IEC 27002:2005 und ISO/IEC 27552). Zudem ist er Professor an der Hochschule Darmstadt für die Themen „Compliance“, „Information Security Management“ und „Sichere Software“. An der Technischen Hochschule Brandenburg betreut er die Fächer „Führung“ und „Business Continuity Management“.

Anzeige

RHENUS DATA OFFICE GMBH

RHENUS LOGISTICS

IHR PARTNER FÜR DATENSCHUTZGERECHTE AKTENVERNICHTUNG
OB AKTENORDNER, CDS, MIKROFICHE ODER MAGNETBANDSPEICHER...

...nach Ablauf der Aufbewahrungsfristen müssen Datenträger sicher entsorgt werden. Vertrauen Sie auf das Leistungspotenzial und Know-How eines seit vielen Jahren führenden Dienstleisters in der Dokumentenlogistik.

- MOBILE UND STATIONÄRE AKTEN- UND DATENTRÄGERVERNICHTUNG
- OFFICE-ENTSORGUNG
- DATENSCHUTZBERATUNG
- DOKUMENTENTRANSPORTE
- AKTENRETTUNG
- RÜCKNAHMELOGISTIK

Erfahren Sie mehr über uns und unsere Dienstleistungen auf www.aktenvernichtung.de

Rhenus Data Office GmbH · Industriestraße 5 · 48301 Nottuln · Tel.: +49 (0)2509 89-0 · info.data-office@de.rhenus.com · www.aktenvernichtung.de

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

EIN JAHR DSGVO

Interview mit Dr. Stefan Brink

Mit dem Start der Datenschutz-Grundverordnung am 25. Mai 2018 stieg der Bedarf an Beratungen extrem an – auch bei den Aufsichtsbehörden. Über ein Jahr Praxiserfahrung DSGVO und die weitere Entwicklung beim Datenschutz sprachen die BvD-News mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink.

BvD-News: Herr Brink, wie sieht es mit Ihrem Stressfaktor aus? Ist nach dem Start der DSGVO mittlerweile etwas Normalität in Ihre Behörde zurückgekehrt?

Stefan Brink: Leider nein. Die Resonanz ist auch nach dem ersten Jahr DSGVO hoch. Nach dem Hype kurz vor und nach dem Start am 25. Mai 2018 ist die Nachfrage auf sehr hohem Niveau stehengeblieben. Insgesamt sind die Anfragen um 30 Prozent gestiegen im Vergleich zu dem Anfrageaufkommen vor der DSGVO. Im privaten Bereich sogar um 50 %.

BvD-News: Wo sehen Sie für Ihre Behörde für die nächste Monate die größten Herausforderungen?

Stefan Brink: Gerade bei der Beratung müssen uns die Parlamente weiter unter die Arme greifen, damit wir weitere Stellen schaffen können. Mit der aktuellen Personalausstattung gelingt es uns nicht mehr, alle Aufgaben wahrzunehmen. Vor allem die Kontrollen müssen deutlich nach oben gefahren werden. Unser Ziel ist es, für das laufende Jahr die Zahl der Kontrollen auf 250 zu erhöhen. 2018 haben ja praktisch keine Kontrollen stattgefunden. Allein bei uns in Baden-Württemberg sind 600.000 verantwortliche Stellen registriert. Mit 250 Kontrollprojekten erreichen wir rund 10.000 verantwortliche Stellen. Diese Kontrollen sind wichtig, um uns einen Überblick zu verschaffen über die Anpassungen bei Firmen und Behörden an die DSGVO. Nicht immer geht es dabei gleich um Sanktionen.

BvD-News: Was ist aus Ihrer Sicht und nach einem Jahr Praxiserfahrung das größte Plus der DSGVO?

Stefan Brink: Einer der Effekte war, dass es viel mehr verantwortliche Stellen gibt, die sich erkennbar um den Datenschutz kümmern. Deren Zahl stieg durch die DSGVO bei uns von 1/3 auf 2/3 an. Sicher waren die Bußgelder, die in der Verordnung verankert sind, ein Treiber dafür. Zudem haben sich viele Unternehmen überhaupt zum ersten Mal intensiv mit den eigenen internen Verfahren zur Erfassung und Verarbeitung von Daten auseinandergesetzt und sich gefragt, was sie überhaupt speichern und wo. Die meisten gehen heute viel bewusster mit der Datenverarbeitung um. Das allein ist schon ein toller Erfolg. Ein großes Plus ist zudem, dass außereuropäische Unternehmen, wenn sie in Europa Dienste anbieten, sich ebenfalls der DSGVO unterwerfen müssen. Dieses Marktortprinzip führt am Ende dazu, dass der vermeintliche Konkurrenznachteil europäischer Firmen zu Unternehmen etwa aus den USA nicht (mehr) existiert.

BvD-News: Und wo sehen Sie das größte Manko?

Stefan Brink: Das liegt für mich darin, dass die DSGVO nicht nach Betriebsform oder Größe von Organisationen unterscheidet. Ihre Pflichten gelten für Facebook genauso wie für kleine Vereine. Das ist keine gute Regelung. Die Dokumentationspflichten zum Beispiel könnten bei einem gemeinnützigen Verein weniger umfassend sein. Das wird sicher auch ein Hauptaspekt bei der Evaluierung der DSGVO 2020 sein. Wissenschaft und Verbände sind ja aufgerufen, Hinweise dazu abzugeben. Und das werden wir in den Evaluationsprozess auf alle Fälle einbringen.

BvD-News: Was empfehlen Sie Unternehmen, Vereinen und Betrieben für die weitere Umsetzung der DSGVO?

Stefan Brink: Vereinen, gemeinnützigen Organisation und solche, die überwiegend mit Ehrenamtlern arbeiten, empfehlen wir, Druck aus dem Kessel zu nehmen. Für meine Behörde kann ich sagen: Wir werden grundsätzlich keine Bußgelder gegen Vereine verhängen. Unternehmen sollten mögliche Kontrollen nicht als Androhung, sondern als Unterstützung verstehen. Unser Ziel ist es, ein gleichmäßiges Anwendungsniveau zu erreichen. Eine Kontrolle kann da helfen herauszufinden, wo es noch hapert. Wir verstehen das als einen gemeinsamen Prozess.

Interview mit

Dr. Stefan Brink
Landesbeauftragter für den Datenschutz
und die Informationsfreiheit Baden-Württemberg

▶ www.baden-wuerttemberg.datenschutz.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

GESETZESÄNDERUNG

EU-STAATEN BESCHLIESSEN NEUES URHEBERRECHT

Nils Steffen

Am 06.06.2019 trat die EU-Richtlinie 2019/790 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt und zur Änderung der Richtlinien 96/9/EG und 2001/29/EG (im Folgenden DSM-Richtlinie) in Kraft. Die Mitgliedsstaaten haben nun Zeit bis zum 07.06.2021, die Bestimmungen der DSM-Richtlinie in nationales Recht umzusetzen.

Dem Erlass der DSM-Richtlinie vorausgegangen waren europaweite öffentliche Proteste. Stein des Anstoßes waren vor allem die kontrovers diskutierten Artikel 15 (im Entwurf noch Artikel 11), der das Leistungsschutzrecht für Presseverleger im Hinblick auf die Online-Nutzung regelt, sowie Artikel 17 (im Entwurf noch Artikel 13), der die Haftung der Online-Diensteanbieter und die sogenannten Upload-Filter betrifft.

Artikel 15 der DSM-Richtlinie

Art. 15 regelt Leistungsschutzrechte bei Presseveröffentlichungen. Presseveröffentlichungen werden definiert als eine Sammlung, die hauptsächlich aus literarischen Werken journalistischer Art besteht, aber auch sonstige Werke oder sonstige Schutzgegenstände enthalten kann. Nicht erfasst werden hingegen Webseiten wie Blogs, deren Inhalte nicht unter der redaktionellen Verantwortung eines Presseverlags bereitgestellt werden.

Die Regelung in Art. 15 spricht den Presseverlegern das ausschließliche Recht der Vervielfältigung, der öffentlichen Wiedergabe und der öffentlichen Zugänglichmachung im Hinblick auf die Online-Nutzung von Presseveröffentlichungen zu. Das bedeutet, dass die in der DSM-Richtlinie genannten Dienstleister wie beispielsweise Suchmaschinen und News-Aggregatoren eine Lizenz einholen müssen, bevor sie die Veröffentlichungen nutzen können. Dadurch wird es Presseverlegern ermöglicht, von den erfassten Dienstleistern Lizenzgebühren zu verlangen, sofern diese ihre Artikel verwenden.

Eine Ausnahme besteht indes bei der Nutzung einzelner Wörter oder sehr kurzer Auszüge aus der Presseveröffentlichung. Ausgenommen ist darüber hinaus die rein private sowie die nicht-kommerzielle Nutzung der Presseveröffentlichungen.

Artikel 17 der DSM-Richtlinie

Bisher konnten sich Plattformen, die online Inhalte zur Verfügung stellten, in Deutschland auf § 8 TMG berufen, wonach diese Diensteanbieter grundsätzlich nicht verantwortlich für fremde Informationen sind, zu denen sie den Zugang zur Nutzung vermitteln.

Art. 17 Abs. 1 der DSM-Richtlinie erklärt die genannten Plattformen nun zu urheberrechtlich Handelnden und Verantwortlichen. Insofern benötigen sie für bei ihnen veröffentlichten Inhalten Lizenzen der Urheber. Fehlt es an der Lizenz, beispielsweise, weil sie verweigert wird oder der Inhaber der Urheberrechte nicht ermittelbar ist, ist der Inhalt illegal und die Plattform selbst für den Verstoß verantwortlich.

Sie haftet nur dann nicht, wenn nachweislich mehrere Bedingungen erfüllt werden. So muss sie sich intensiv um die Lizenz bemüht haben, illegale Inhalte mittels »hoher branchenüblicher Standards« blocken und illegale Uploads nach Kenntnis sofort sperren bzw. entfernen. Die Mittel lässt die Richtlinie offen, allerdings ist hier der Raum für Upload-Filter gegeben, denn die Richtlinie verlangt zusätzlich, dass alle Anstrengungen unternommen werden um das künftige Hochladen des bekannten illegalen Uploads zu verhindern.

Diese Verpflichtung betrifft alle Plattformen, die länger als 3 Jahre am Markt sind und einen Jahresumsatz von mehr als 10 Mio. Euro haben. Hat die Plattform mehr als 5 Mio. Benutzer, muss sie den Nachweis erbringen, dass sie alle Anstrengungen unternommen hat, um das künftige Hochladen der gemeldeten Inhalte zu verhindern.

Aussicht

Das neue Leistungsschutzrecht für Presseverleger kann durchaus als Meilenstein auf dem Weg zu einer angemessenen Vergütung im digitalen Zeitalter betrachtet werden. Offen bleibt jedoch, wie weit die Ausnahme für einzelne Wörter oder sehr kurze Auszüge reicht. Die Auslegung wird wohl erst durch die Gerichte erfolgen, sodass es noch dauern wird, bis hier Rechtssicherheit besteht.

Die Vorschrift des Art. 17 wirft hingegen weiterhin eine Menge Fragen auf, die sich weder durch die Erwägungsgründe noch durch die noch zu erlassenen Leitlinien klären lassen werden. So bleibt unter anderem offen, was unter »hohen branchenüblichen Standards« zu verstehen ist. Einer der größten Kritikpunkte an Art. 17 ist aber weiterhin, dass es infolge des Einsatzes von Upload-Filtern zu einer ungewollten Sperrung legitimer Inhalte kommen kann. Zwar sieht die Richtlinie ausdrücklich vor, dass die Zusammenarbeit zwischen den Plattformen und den Inhabern der Urheberrechte nicht bewirken darf, dass die rechtmäßige Nutzung eigentlich legitimer Inhalte beeinträchtigt wird, und nicht zur Sperrung von solchen Inhalten führen darf. Gleichwohl besteht die größte Herausforderung für die betroffenen Plattformen darin, angesichts des neuen Haftungsrisikos den Verpflichtungen gerecht zu werden und gleichzeitig sicherzustellen, dass rechtmäßig hochgeladene Inhalte nicht blockiert werden.

Zuletzt bleibt festzuhalten, dass die DSM-Richtlinie noch der Umsetzung in nationales Recht bedarf und dem nationalen Gesetzgeber durch die Richtlinie ein gewisser Spielraum zur Verfügung steht, diese nicht wortgetreu umzusetzen. Aus Regierungskreisen hieß es deshalb auch bereits, dass möglichst auf den Einsatz von Upload-Filtern verzichtet werden soll. Stattdessen - so der Vorschlag der CDU - sollen durch gesetzlich verpflichtende Pauschallizenzen und eine zeitlich begrenzte Lizenzgebührenfreiheit Upload-Filter obsolet werden.

Über den Autor

Nils Steffen
Rechtsanwalt, Datenschutzbeauftragter (TÜV) und ESCA Legal Auditor, Derra, Meyer & Partner Rechtsanwälte PartGmbB
Nils Steffen berät seit 2016 europaweit nationale und internationale Unternehmen in den Beratungsfeldern Datenschutz, Wettbewerbs- und Urheberrecht. Die Beratung umfasst die außergerichtliche und gerichtliche Vertretung, auch gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, sowie Vertragsgestaltungen. Er ist Referent verschiedener Datenschutzveranstaltungen, Autor von Fachbeiträgen zum Datenschutzrecht, Mitautor der Zeitschrift »Datenschutz digital« und ESCA Legal Auditor.

▶ www.derra.eu

DERRA, MEYER & PAR
Rechtsanwälte PartGmbB

IHNEN STEHT EIN UPDATE FÜR IHRE DATENSCHUTZRECHTLICHE EINWILLIGUNG ZUR VERFÜGUNG!

Dr. Carlo Piltz und Melanie Pradel

Die Einwilligung empfinden viele Verantwortliche immer noch als die angenehmste Rechtsgrundlage für eine Datenverarbeitung. Dort, wo es möglich (nicht nötig!) erscheint, wird von der betroffenen Person eine Einwilligung eingeholt. Auf die »Anforderungen an die datenschutzrechtliche Wirksamkeit der Einwilligung« ist Prof. Dr. Taeger in der letzten Ausgabe der BvD-News (Ausgabe 1/2019) bereits ausführlich eingegangen. Doch die Praxis im Datenschutzrecht ist schnelllebig und kurzweilig. Gerichtsurteile, Hinweise der Aufsichtsbehörden und deren Tätigkeitsberichte werden derzeit in sehr kurzen zeitlichen Abständen veröffentlicht. Für einen Einblick in die aktuellen Diskussionen rund um die datenschutzrechtliche Einwilligung aus den Veröffentlichungen dient Ihnen der folgende Artikel.

»Eine Übermittlung Ihrer Gesundheitsdaten an Dritte erfolgt bei uns unverschlüsselt, einverstanden?«

So ähnlich zumindest hat eine Allergie-Tagesklinik in Österreich einen Teil der Einwilligungserklärung für die Verarbeitung ihrer Patientendaten formuliert. Die Einwilligung zur Datenverarbeitung mit der Zustimmung zur unverschlüsselten Übermittlung an »relevante Dritte« zu verbinden, sah die zuständige österreichische Aufsichtsbehörde allerdings nicht gern. Sie erklärte diese Einwilligung als unwirksam. Eine Einwilligung von der betroffenen Person kann nur für eine Datenverarbeitung erteilt werden. Also nur im Rahmen des Art. 6 bzw. Art. 9 DSGVO als Rechtsgrundlage dienen. Die Betroffenen können aber, nach Ansicht der Behörde, nicht in für sie negativ abweichende Sicherheitsstandards (hier eine Abweichung von den Vorgaben des Art. 32 DSGVO) einwilligen.

Auch ein anderer Teil der Einwilligungserklärung widersprach nach Auffassung der Aufsichtsbehörde den Anforderungen an die Datensicherheit. Demnach sollte die betroffene Person zur Kenntnis nehmen, »dass durch die Übermittlung der Daten (unberechtigte) Dritte Kenntnis über die Informationen erhalten können und diese Daten verändert werden können«. Sie sollte sich zudem bewusst zeigen, »dass dies zur Offenlegung […] [ihres] Gesundheitszustandes führen kann […] [und] dass die Allergie-Tagesklinik D*** keinerlei Haftung für die korrekte und vollständige Übermittlung der Daten übernehmen kann«. Von dem gesetzlichen vorgegebenen Schutzniveau (Art. 32 DSGVO) könne aber nach Auffassung der Datenschutzbehörde nicht durch Einwilligung der betroffenen Person abgewichen werden. Nach Ansicht der Aufsichtsbehörde sind die Anforderungen an die Sicherheit der Verarbeitung nach Art. 32 DSGVO also mithin objektiv erfüllt oder nicht. Eine Einwilligung des Betroffenen könne dabei nicht berücksichtigt werden.

Zudem ersuchte die Tagesklinik eine Zustimmung in Form einer unwiderruflichen Einwilligung der Patienten darin, dass Auftragsverarbeiter bei der Verarbeitung der patientenbezogenen Daten herangezogen werden dürfen (*»Ich stimme weiters unwiderruflich zu, dass die Allergie-Tagesklinik D*** jederzeit andere Unternehmen und/oder Personen zur Durchführung der vereinbarten Dienstleistung heranziehen darf. Dies betrifft auch die Verarbeitung inkl. Speicherung von personenbezogenen Daten.«*). Nicht nur die Unwiderruflichkeit verstößt gegen Art. 7 Abs. 3 DSGVO, auch mit der Zustimmung zur Auftragsverarbeitung ist die Aufsichtsbehörde nicht einverstanden. Die Pflicht zur sorgfältigen Auswahl und zum Abschluss eines Auftragsverarbeitungsvertrages trifft allein den Verantwortlichen und kann nicht mit der Zustimmung der betroffenen Person aufgehoben oder abgewälzt werden.

Die datenschutzrechtliche Einwilligung ist, zumindest nach Ansicht auch anderer Aufsichtsbehörden, kein Allheilmittel gegen die aus der DSGVO erwachsenen Pflichten. Sie kann nicht für jeden Umstand der Verarbeitung eingeholt werden, um die praktische und möglicherweise fehlerhafte Umsetzung der DSGVO zu legitimieren. Nach Ansicht der österreichischen Aufsichtsbehörde ist sie auf die Zustimmung zur ursprünglichen Verarbeitung personenbezogener Daten begrenzt.

»Wollen Sie das heute mit Ihren Daten bezahlen?«

Viele Dienstleistungen werden den Nutzern im Internet kostenlos angeboten. Man müsse nur schnell seine Daten in das Eingabefeld eintragen und deren Nutzung für Werbezwecke zustimmen. Doch damit wird das »kostenlos« eher zum Bezahlen mit Daten und erinnert manch einen Datenschutzrechtler an eine unzulässige Kopplung der Einwilligung an eine davon separat zu betrachtende Verarbeitung nach Art. 7 Abs. 4 DSGVO. Das Bayerische Landesamt für Datenschutzaufsicht (»BayLDA«) hat sich in seinem aktuellen 8. Tätigkeitsbericht zu diesem Geschäftsmodell geäußert und Stellung zu der Frage bezogen, ob es unter Geltung der DSGVO noch rechtmäßig ist oder »wegen einer nicht freiwillig erteilten Einwilligung zur Verarbeitung« eben gegen das Kopplungsverbot verstößt. Nach Auffassung des BayLDA liegt kein Verstoß vor. Hier ist die vertragliche Rechtsgrundlage zur Datenverarbeitung (Art. 6 Abs. 1 lit. b) DSGVO) auch für den Umgang mit Daten für werbliche Zwecke einschlägig, so dass eine Zustimmung nicht erforderlich ist. Die Datenverarbeitung nach Art. 6 Abs. 1 lit. b) DSGVO ist in den vorliegenden Fällen aber nur dann rechtmäßig, »wenn die ausbedungene Gegenleistung des Nutzers, d. h. die Zustimmung zur Verarbeitung seiner Daten für die Zusendung eines Werbe-Newsletters, bei Vertragsabschluss über die vereinbarte kostenlose Dienstleistung klar und verständlich dargestellt wird und damit ein Nutzer eine sachgerechte Entscheidungsgrundlage hat«.

Eine ähnlich gelagerte Geschäftskonstellation beschäftigte die österreichische Datenschutzaufsichtsbehörde (»DSB«). Für das Online-Angebot einer Tageszeitung musste sich der Nutzer entscheiden: Entweder stimmt er der Datenverarbeitung zu Werbezwecken zu und er erhielt »kostenlos« Zugang zu dem Online-Auftritt, oder er muss ein kostenpflichtiges Abonnement der Zeitung abschließen und es findet keine Datenverarbeitung in Form von Tracking über Cookies und durch Webanalysetools statt. Auf die darauf bezogene Beschwerde eines Nutzers, dies verstoße gegen das Kopplungsverbot der DSGVO, entschied sich die DSB gegen ein striktes Kopplungsverbot und sprach sich für einen Ermessenspielraum auf Seiten des Verantwortlichen aus. Das Kopplungsverbot soll Nachteile für die betroffene Personen verhindern, die in Form einer Täuschung, Einschüchterung, Nötigung oder einer beträchtlichen negativen Folge vorliegen können. Eine solche beträchtliche negative Folge bzw. einen wesentlichen Nachteil sieht die DSB in dem alternativen Abonnement, das monatlich 6 Euro beträgt, allerdings nicht. Das »Bezahlen mit Daten«, um auf das Online-Angebot der Tageszeitung zugreifen zu können, verstoße nicht gegen das Kopplungsverbot.

»Weisen Sie mir doch bitte mal nach, dass ich Cookies wollte!«

Viel Unsicherheiten und dementsprechend viele Veröffentlichungen beziehen sich auf die sog. Cookie-Banner auf Websites. Allgemein geht es um die Einholung einer Einwilligung des ▸

Besuchers für die Datenverarbeitung zu Werbezwecken. Davon erfasst sind insbesondere das Setzen von Cookies und die Verarbeitung der Nutzerdaten durch Webanalysetools. Für die Rechtmäßigkeit von Cookie-Bannern legt die Datenschutzkonferenz (»DSK«) nun in ihrer »Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien« folgende Richtwerte fest:

- Das Banner soll eine Übersicht aller einwilligungsbedürftigen Verarbeitungsvorgänge, Nennung der beteiligten Akteure und deren Funktion und Auswahlmenü zur Aktivierung enthalten.
- Die Erfassung der Nutzerdaten ist solang zu blockieren, bis die Einwilligung wirksam erteilt wurde.
- Jederzeitige Zugriffsmöglichkeit auf Impressum und Datenschutzerklärung muss bestehen.
- Es ist eine aktive Handlung des Nutzers notwendig: z.B. Setzen eines Häkchens oder Klick auf eine Schaltfläche.
- Die getroffene Entscheidung des Nutzers kann von Verantwortlichem auf dem Endgerät für den Fall eines weiteren Aufrufs der Website gespeichert werden.
- Es ist eine einfache Widerrufsmöglichkeit zu implementieren (iSd Art. 7 Abs. 3 S. 4 DSGVO).

Das klingt für die Umsetzung zwar zunächst aufwendig. Was derzeit die Praxis allerdings noch mehr beschäftigt, ist die Nachweismöglichkeit dieser Einwilligung der Nutzer. Es geht auch um die technische Umsetzung der Nachweispflicht des Verantwortlichen nach Art. 7 Abs. 1 DSGVO. Die dem Website-Betreiber offengelegte IP-Adresse des Nutzers stellt »ein datenschutzrechtlich relevantes Datum« dar, so das BayLDA. Nach Auffassung der DSK in der oben genannten Orientierungshilfe und des BayLDA ist es »[z]ur Erfüllung der Nachweispflichten des Art. 7 Abs. 1 DSGVO […] gem. Art. 11 Abs. 1 DSGVO nicht erforderlich, dass die Nutzer dazu direkt identifiziert werden. Eine indirekte Identifizierung (vgl. ErwGr. 26) ist ausreichend«. Diese indirekte Identifizierung kann nur durch die Speicherung der IP-Adresse möglich sein.

Fazit

Auch wenn die Einholung einer Einwilligung für den Verantwortlichen zunächst am einfachsten scheint, bietet diese Rechtsgrundlage viele Hürden. Insbesondere werden diese erst in der Anwendung der DSGVO deutlich und diskutiert. Der Verantwortliche hat sich an die engen Grenzen von Art. 6 Abs. 1 lit. a) und Art. 7 DSGVO zu halten. Zudem ist stets das über der Datenverarbeitung schwebende Damoklesschwert der jederzeitigen Widerrufsmöglichkeit nach Art. 7 Abs. 3 DSGVO zu beachten. Vielleicht tut ein Verantwortlicher das, weil die Einwilligung den Schein des vorrangigen Erlaubnistatbestandes aus Art. 6 Abs. 1 DSGVO in sich birgt. Doch so ist es eben nicht. Die DSGVO sieht in Art. 6 Abs. 1 kein Rangverhältnis der Erlaubnistatbestände vor. Auch die DSK hat klargestellt: »Sämtliche Erlaubnistatbestände der DSGVO sind als gleichrangig und gleichwertig zu betrachten«. Eine Einwilligung ist für manche Datenverarbeitungen erst gar nicht erforderlich. Eine sorgfältige, rechtliche Prüfung der Datenverarbeitung ermöglicht die Heranziehung anderer Erlaubnistatbestände und umgeht somit die derzeitigen und noch kommenden Umsetzungsschwierigkeiten bei der Einholung und Nachweisbarkeit einer Einwilligung.

Über die Autoren

Dr. Carlo Piltz

ist Rechtsanwalt und Salary Partner bei reuschlaw Legal Consultants in Berlin und leitet dort das Team Cybersecurity & Datenschutz.

Melanie Pradel

ist wissenschaftliche Mitarbeiterin im Team Cybersecurity & Datenschutz bei reuschlaw Legal Consultants in Berlin.

▶ www.reuschlaw.de

reuschlaw
Legal Consultants

Anzeige

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

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

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

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

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

DATENSCHUTZPRAXIS

DATENSCHUTZ IM UNTERNEHMEN: CLOUD VS. ON-PREMISE

Philip Kissi

Bei der Einrichtung der IT-Infrastruktur eines Unternehmens gibt es zwei ganz unterschiedliche Herangehensweisen. Es ist möglich, die Dienste On-Premise – also auf Servern innerhalb der eigenen Firmengebäude – zur Verfügung zu stellen. Eine andere Alternative besteht darin, eine Cloud zu verwenden. Dabei stellt ein spezialisierter Dienstleister alle erforderlichen Dienste zur Verfügung. Der Zugang findet über das Internet statt. Im Geschäftsalltag erfahren wir jedoch hin und wieder Bedenken zu Cloud Lösungen. Interessenten äußern vereinzelt die Befürchtung, dass ihre Unternehmensdaten in der Cloud nicht sicher seien oder dass sie damit nicht die Anforderungen der Datenschutzgrundverordnung (DSGVO) erfüllen. Diese Einwände waren der Anlass, Cloud und On-Premise Lösungen hinsichtlich Datensicherheit und Datenschutz für Unternehmen zu vergleichen.

Der technische Hintergrund: Unterschiede zwischen Cloud und On-Premise

Die traditionelle Form der IT-Infrastruktur in einem Unternehmen besteht darin, innerhalb des eigenen Firmengebäudes einen Server zu installieren. Diese Vorgehensweise wird als On-Premise bezeichnet. Das bedeutet übersetzt etwa an Ort und Stelle oder im Gebäude. Das Unternehmen kann dabei genau die Hardware auswählen, die es benötigt. Auch die installierten Betriebssysteme und Programme kann es an seinen Bedürfnissen ausrichten. Die andere Alternative besteht darin, diese Aufgabe in die Cloud auszulagern.

Doch auch hierbei gibt es unterschiedliche Herangehensweisen. Eine Möglichkeit besteht in Infrastructure as a Service (IaaS). Das bedeutet, dass der Kunde Zugang zur Hardware erhält – beispielsweise zu einem Server oder zu einem Datenspeicher. Wie er diese Infrastruktur nutzt, bleibt jedoch dem Kunden überlassen. Platform as a Service (PaaS) bedeutet hingegen, dass der Cloud-Anbieter dem Kunden eine Laufzeitumgebung zur Verfügung stellt. Die Rechen- und Speicherkapazitäten lassen sich dabei dynamisch an die Anforderungen anpassen. Hier kann der Kunde dann seine eigenen Programme ausführen. Das umfassendste Konzept ist Software as a Service (SaaS). Dabei stellt der Cloud-Anbieter genau das Programm bereit, das der Kunde benötigt. Dieser muss es lediglich anwenden. Um alle anderen Aufgaben kümmert sich der Cloud-Dienstleister.

Cloud und On-Premise: die Vor- und Nachteile der verschiedenen Systeme

Sowohl Cloud- als auch On-Premise-Lösungen bieten einige Vor- und Nachteile. Die Verwendung eines eigenen Firmenservers zeichnet sich dadurch aus, dass der Anwender die volle Kontrolle über das System behält. Er kann selbst festlegen, welche Hardwareausstattung er anschafft, welche Software er verwendet und welche Vorkehrungen er für die Datensicherheit und den Datenschutz trifft. Es ist möglich, die Systeme genau an die Anforderungen anzupassen und dabei auch Angebote unterschiedlicher Hersteller miteinander zu kombinieren. Dennoch muss der Anwender selbst dafür Sorge tragen, dass die technischen Voraussetzungen gegeben sind, wie beispielweise aktuelle Hardware, sowie regelmäßige Updates, um die Sicherheit gewährleisten zu können. Dieses ist zeitaufwendig und kostspielig.

Bei Cloud-Lösungen hat der Anwender hingegen eine etwas geringere Entscheidungsfreiheit. Insbesondere im Bereich der Sicherheit ist er darauf angewiesen, dass der Dienstleister diese Aufgabe zuverlässig erfüllt, ohne jedoch selbst darauf Einfluss nehmen zu können. Doch bietet auch diese Alternative viele Vorteile. An erster Stelle steht dabei, dass bei der Nutzung der Cloud keine Investitionskosten anfallen. Darüber hinaus sind keine Mitarbeiter für die Wartung der IT-Infrastruktur erforderlich. Da viele Unternehmen Schwierigkeiten damit haben, qualifizierte IT-Fachkräfte zu finden, stellt das eine enorme Erleichterung dar. Darüber hinaus kann die Nutzung der Cloud Risiken minimieren. Wenn ein Firmenserver ausfällt, muss das entsprechende Unternehmen selbst für die daraus entstandenen Schäden aufkommen. Wenn hingegen ein Cloud-Dienstleister beauftragt wird, ist dieser haftbar, wenn er die vertraglichen Zusagen nicht einhält.

Cloud-Lösungen werden in Unternehmen immer beliebter

Diese Vorteile führen dazu, dass sich immer mehr Unternehmen für die Nutzung der Cloud entscheiden. Eine Studie von bitkom research und KPMG kam zu dem Ergebnis, dass im Jahre 2017 bereits 66 Prozent der Unternehmen in Deutschland das Cloud Computing nutzten. Hinzu kamen 21 Prozent, die diese Möglichkeit diskutierten oder bereits konkret planten. Nur zwei Jahre zuvor waren die Werte noch deutlich niedriger. 2015 nutzten 54 Prozent der Unternehmen Cloud-Dienste und 18 Prozent planten oder diskutierten deren Nutzung[1]. Beispielsweise konnte der deutsche Softwarehersteller SAP in 2018 einen höheren Umsatz mit seinen Cloud Lösungen erzielen, als mit seinen On-Premise Lösungen. All das zeigt auf, dass die Nutzung der Cloud immer beliebter wird.

Cloud-Service-Provider oder Cloud-Nutzer: Wer ist für die Einhaltung der Datenschutzregeln verantwortlich?

Für besonders große Besorgnis bei der Verwendung der Cloud sorgt die Datenschutzgrundverordnung (DSGVO), die 2018 anwendbar geworden ist. Diese setzt strenge Regeln für den Umgang mit personenbezogenen Daten und droht mit hohen Strafen. Die erste Frage, die sich bei der Nutzung der Cloud stellt, besteht darin, wer für die Einhaltung der Regeln verantwortlich ist – der Cloud-Dienstleister oder der Kunde. Die Antwort darauf ist eindeutig: beide. Die Verordnung der EU unterscheidet zwischen dem Datenverantwortlichen (also dem Cloud-Nutzer) und dem Datenverarbeiter (also dem Cloud-Dienstleister). Für beide gelten genaue Vorschriften. Der Kunde kann nicht einfach alle Anforderungen zum Datenschutz an den Cloud-Dienstleister übertragen. In erster Linie ist er dazu verpflichtet, zu überprüfen, ob der Anbieter alle Regelungen einhält.

Dokumentation der Datenspeicherung

Einer der wesentlichen Bestandteile der DSGVO besteht darin, dass die Unternehmen die Speicherung der personenbezogenen Daten genau dokumentieren und jederzeit Auskunft darüber geben können müssen. Daraus folgt, dass der Cloud-Kunde beim Vertragsabschluss genaue Compliance-Regelungen aufstellen muss. Das bedeutet, dass er sich mit dem Cloud-Anbieter absprechen muss, wer für diese Aufgabe verantwortlich ist. Eine weitere Anforderung der DSGVO besteht darin, dass die Unternehmen das ausdrückliche Einverständnis der Betroffenen ▶

[1] https://www.bitkom.org/Presse/Presseinformation/Zwei-von-drei-Unternehmen-nutzen-Cloud-Computing.html

für die Datenspeicherung abfragen müssen. Auch hierbei gilt es abzuklären, wer für diese Aufgabe verantwortlich ist – der Cloud-Dienstleister oder der Kunde.

Der Standort der Cloud-Server

Ein weiteres Problem, das bei der Nutzung der Cloud Probleme bereiten kann, ist der Standort der Server. Die DSGVO verbietet es, personenbezogene Daten von EU-Bürgern in Ländern abzuspeichern, in denen kein ausreichender Schutz gewährleistet ist. Es obliegt dem Datenverantwortlichen – also dem Cloud-Kunden – auf diesen Aspekt zu achten. Daher ist es empfehlenswert, einen Anbieter auszuwählen, der ausschließlich Rechenzentren in Europa betreibt.

Die Sicherheit der Daten

Das Unternehmen, das die personenbezogenen Daten erhebt, ist auch für deren Sicherheit verantwortlich. Wenn ein Hacker die Informationen entwendet, kann es dafür haftbar gemacht werden. Daher ist es wichtig, einen Anbieter mit einem sicheren Rechenzentrum auszuwählen. Außerdem ist es wichtig, auf einen sicheren Übertragungsweg zu achten. Damit Angreifer die Informationen nicht bereits bei der Übertragung in die Cloud abfangen können, sollten sie schon während der Übermittlung verschlüsselt sein.

Tipps für den Umgang mit personenbezogenen Daten in der Cloud

Die Vorgaben der DSGVO und die Nutzung der Cloud schließen sich nicht gegenseitig aus. Allerdings ist es für eine datenschutzkonforme Speicherung in der Cloud notwendig, einige Regeln zu beachten. Die folgenden Tipps helfen Ihnen dabei, Probleme mit der DSGVO zu verhindern:

1. Ernennen Sie zunächst einen fachkundigen Datenschutzbeauftragten, der die Einhaltung aller Regeln überprüft.
2. Vergewissern Sie sich beim Anbieter, ob die Daten gesetzeskonform gespeichert werden. Halten Sie dabei alle Details vertraglich fest. Das sorgt für eine gute Absicherung.
3. Klären Sie ab, ob der Dienstleister den Dokumentations- und Informationspflichten nachkommt. Halten Sie auch diese Vorgaben vertraglich fest.
4. Achten Sie bereits bei der Übertragung der Daten auf eine sichere Verschlüsselung.
5. Wählen Sie einen Anbieter aus, der seine Server innerhalb der EU betreibt.
6. Achten Sie auf einen Anbieter mit einem sicheren Rechenzentrum – am besten mit Zertifizierung nach ISO27001.
7. Überarbeiten Sie Ihre Datenschutzerklärung und passen Sie diese so an, dass sie auch zur Nutzung von Cloud-Diensten passt.

Fazit: Cloud-Lösungen ermöglichen einen zuverlässigen Datenschutz

Als Fazit kann man festhalten, dass sich die Nutzung der Cloud und eine gesetzeskonforme Datenspeicherung nach DSGVO nicht gegenseitig ausschließen. Auch in der Cloud ist es möglich, die Daten so abzuspeichern, dass sie den Anforderungen dieser Verordnung entsprechen. Allerdings passiert das nicht automatisch. Wenn Sie sich zur Nutzung der Cloud entschließen, werden Sie nicht von allen Pflichten entbunden. Eine ständige Kontrolle der Vorgaben und eine vertragliche Regelung zur Übernahme der Aufgaben sind sehr wichtig.

Über den Autor

Philip Kissi
Marketing & Communications Specialist bei WorkforceIT GmbH

Über WorkforceIT GmbH
Die WorkforceIT GmbH bietet verschiedene Cloud-Dienstleistungen an. Ein Beispiel hierfür ist Speakap – ein Service für eine einfache und effiziente interne Kommunikation im Unternehmen. Darüber hinaus bieten wir Appical an. Dabei handelt es sich ebenfalls um eine Mitarbeiter-App, die das Onboarding neuer Mitarbeiter erleichtert. Beide Angebote tragen daher zu einem effizienten Workforce Management bei.

WorkforceIT GmbH
Kaiser-Wilhelm-Ring 27-29, 50672 Köln

- www.workforce-it.com/de
- info@workforce-it.de
- Tel: +49 (0)221 5694407

Anzeige

DIE DIGITALE TRANSFORMATION BRAUCHT NEUE SECURITY-STANDARDS.

INDUSTRIE 4.0 UND IoT NEUE MÖGLICHKEITEN BERGEN NEUE GEFAHREN.

IT taucht immer dort auf, wo das Geschäft stattfindet. Das heißt, alle User, Applikationen und Daten sind ständig in Bewegung. Agilität und Flexibilität gewinnen gegenüber der Stabilität immer mehr an Bedeutung. IT Security wird nicht mehr durch einen konkreten Ort definiert. Deshalb muss Security überall dort sein, wo immer IT stattfindet.

Das gilt heute besonders für das IoT in der Industrie und Wirtschaft. Ob Supermärkte, Geldautomaten oder ganze Airlines – wer die Effizienz der Technologie nutzen will, muss wissen, wie er sie schützen kann. Denn dort, wo ein derartiges Effizienzpotenzial liegt, finden sich unzählige Gefahrenpotenziale für die Sicherheit. Hierbei können existenzbedrohende Risikofaktoren entstehen. Das „Internet of Things“ ist auf die „Security of Things“ angewiesen.

Genau hierfür bietet DREGER IT Lösungen an, die höchste Sicherheit und echte Mehrwerte für Ihr Unternehmen gewährleisten.

Darüber hinaus profitieren Sie von Mehrwerten und Services, die individuell auf die Bedürfnisse Ihres Unternehmens zugeschnitten sind.

D-BUSINESS®
MONITORING
IHR MEHRWERT DURCH PROAKTIVE FEHLERERKENNUNG.

Ziel des D-BUSINESS® Monitoring ist es, Ihre IT-Abteilung zu unterstützen und für höchste Sicherheit zu sorgen. Es soll einen reibungslosen Betrieb Ihrer Infrastrukturen, Betriebssysteme und Anwendungen gewährleisten.

D-BUSINESS®
MANAGED SECURITY
IHR MEHRWERT DURCH EIN SOLIDES SICHERHEITSFUNDAMENT.

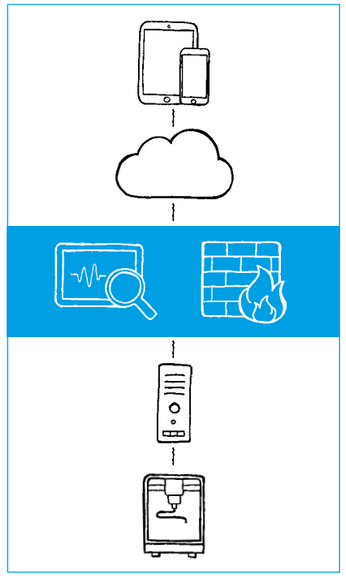
Mit dem richtigen Konzept können Sie die Sicherheit Ihrer Infrastruktur auf ein solides Fundament stellen. Unzureichend geschützte Informationen sind ein häufig unterschätzter Risikofaktor, der existenzbedrohend werden kann. Dabei sind ein vernünftiger Informationsschutz und die Grundsicherung der IT schon mit verhältnismäßig geringen Mitteln zu erreichen.

D-BUSINESS®
MANAGED IoT
UNSERE LÖSUNGEN FÜR IHRE IoT-INFRASTRUKTUR.

Mit den Produkten D-BUSINESS® Monitoring und D-BUSINESS® Managed Security erreichen Sie für Ihre IoT-Infrastruktur maximale Sicherheitsstandards bei einer gleichzeitig hohen Entlastung für die IT-Abteilung Ihres Unternehmens.

DREGER IT gewährleistet:

- Sichere Konnektivität und Überwachung der Geräte
- Erhöhung der Sicherheit durch Mikrosegmentierung, Isolierung von potenziell unsicheren Gräten
- Bedienung durch Nicht-IT-Personal (Fachabteilungen) möglich, daher keine zusätzliche Belatung der IT-Abteilung
- Reduzierung bzw. Beschleunigung des Wartungsaufwands für den Betrieb von IoT-/Industrielösungen



DREGER IT bietet Ihnen mit über 25 Jahren Erfahrung in der IT Branche, zuverlässige Services bei höchstem Datenschutz. Das beinhaltet mandantenfähige Cloud Services ohne lange Vertragsbindungen mit individuell angelegten Infrastrukturen. Zudem stehen Plattformen oder Anwendungen mit der Option auf Überwachung und Support modular zur Verfügung.

Das DREGER IT Rechenzentrum stellt Ihnen eine Vielfalt standardisierter modularer Komponenten bereit, die je nach Anforderung individuell zusammengestellt und anpassbar sind. Sie entscheiden hierbei, wie viel Verantwortung Sie an DREGER IT abgeben möchten.

DREGER Consulting GmbH & Co. KG
Hanauer Landstraße 182a
60314 Frankfurt am Main
Telefon: 069-90479-0
info@dreger.de

www.dreger.de
www.folderflex.de

DATENSCHUTZPRAXIS

INTERVIEW MIT DEM FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE ZUM THEMA „VOLKSVERSCHLÜSSELUNG“

Michael Herfert und Jürgen Hartz

Hartz: Die fehlende sichere Verschlüsselung, während der E-Mail Verkehr ständig steigt, ist immer noch eine große Schwachstelle der elektronischen Kommunikation, nicht nur im privaten Bereich, sondern auch im geschäftlichen. Selbst viele Unternehmen versenden vertrauliche Informationen als offene E-Mail oder Dokumente, selbst mit sensiblen geschäftlichen oder gar Gesundheitsdaten, als unverschlüsselte Anlage.

Warum sind nach Ihrer Meinung die E-Mail Nutzer so wenig auf die Sicherheit beim E-Mail Verkehr bedacht?

Herfert: IT-Sicherheit entzieht sich der unmittelbaren Wahrnehmung. Wenn man mit seinem Web-Browser im Internet unterwegs ist, dann ist das Erlebnis unabhängig davon, ob der Browser eine sichere Verbindung über das TLS-Protokoll aufgebaut hat oder nicht. Ein Textverarbeitungsprogramm, das hellgraue Schrift vor einem weißen Hintergrund zeigt, würde niemand benutzen, weil die Mängel gravierend sind und unmittelbar wahrgenommen werden. Mängel in der IT-Sicherheit manifestieren sich oft erst viel später, etwa dann, wenn Firmengeheimnisse verloren gegangen sind oder personenbezogene Daten in falsche Hände geraten sind.

Hartz: Der neue elektronische Personalausweis, der verschiedene Zusatzfunktionen zum Beispiel für den elektronischen Einkauf beinhaltet, hat im Gegensatz zu anderen Ländern, die dies bei der Neueinführung von Ausweisdokumenten berücksichtigt haben, keine Möglichkeit, Dokumente zu verschlüsseln.

War die technische Hürde für die Installation eines sicheren E-Mail Zertifikates wie PGP oder S/MIME einfach zu hoch oder zu teuer?

Herfert: Ich bin ein großer Freund des neuen Personalausweises. Gerade in Bezug auf Datenschutz ist er vorbildlich. Es ist technisch möglich, ein S/MIME Zertifikat für eine digitale Signatur nachzuladen. Dafür gibt es zurzeit keinen Anbieter. Die Fähigkeit, Dokumente zu verschlüsseln, erhielte er aber auch dadurch nicht. Der neue Personalausweis entwickelt sich ja immer weiter, wer weiß was die Zukunft bringt.

Hartz: Das Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt hat zusammen mit der Telekom AG mit dem Projekt »Volksverschlüsselung« eine Initiative gestartet, eine sichere Verschlüsselung für »jedermann« bereitzustellen. Der BvD hat in seinen Fortbildungen bereits vor Jahren Seminarangebote zur Verschlüsselung inklusive Ausgabe eines persönlichen S/MIME-Zertifikates durchgeführt. Datenschutzbeauftragte sollten aufgrund ihrer Aus- und Weiterbildung über Mindestkenntnisse im IT-Bereich verfügen. Dennoch war nicht für alle die Installation des persönlichen Zertifikates unproblematisch. Offensichtlich stellt der Einsatz von sicherer Verschlüsselungstechnik mittels Zertifikaten, die ja in die Browser bzw. Mailprogramme eingebunden werden müssen, die Anwender vor Probleme.

Wie haben Sie diese Herausforderung umgesetzt?

Herfert: Wir haben mit der Volksverschlüsselungs-App eine Applikation für Microsoft Windows programmiert, die dem Nutzer alle schwierigen Schritte abnimmt. Er muss seine Mail-Adresse eingeben und einen Registrierungscode, den er zuvor von uns im Rahmen einer Identitätsfeststellung erhalten hat, und schon hat er Schlüssel sowie Zertifikate und sie sind auf seinem Rechner dort gespeichert, wo sie von den Applikationen erwartet werden. Es sind keinerlei weitere Konfigurationsschritte erforderlich. Die Schlüssel sind unmittelbar nutzbar.

Die Anforderung nach maximal einfacher Benutzbarkeit war von Anfang an ein hochpriorisiertes Ziel. Es war uns klar, dass wir als Informatiker das Erreichen dieses Ziels nicht selber beurteilen können. So haben wir wiederholt Nicht-Informatiker in den Entwicklungszyklus eingebunden, um tatsächlich »Usability by Design« zu erhalten.

Hartz: Können Sie uns in einfachen Worten erklären, warum das Zertifikat durch das Fraunhofer SIT eine wirklich sichere Möglichkeit der E-Mail Verschlüsselung darstellt?

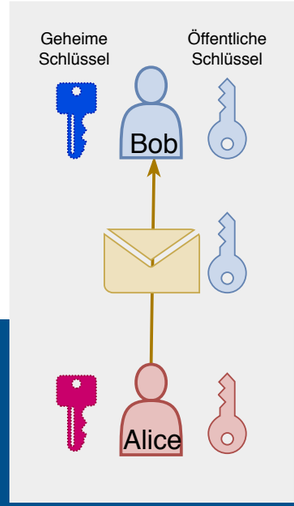


Abb.: Asymmetrische Verschlüsselung: Jeder Nutzer besitzt 2 Schlüssel,einen geheimen (links) und einen öffentlichen (rechts). Alice verwendet Bobs öffentlichen Schlüssel, um eine Nachricht für ihn zu verschlüsseln. Nur Bob kann sie mit seinem geheimen Schlüssel wieder entschlüsseln.

Herfert: Wir stellen nur dann ein Zertifikat aus, wenn wir uns von der Identität des Nutzers anhand eines Ausweisdokuments überzeugt haben. Auf das Übersenden einer Ausweiskopie oder gar die reine Überprüfung einer Mailadresse lassen wir uns nicht ein. Wer ein Zertifikat der Volksverschlüsselung nutzt, etwa über unseren Verzeichnisdienst, kann sicher sein, dass hinter diesem Zertifikat tatsächlich die im Zertifikat genannte Person steht.

Die eigentliche Verschlüsselung geschieht auf Basis etablierter, vollständig offen gelegter kryptografischer Algorithmen, die seit vielen Jahren im allgemeinen Gebrauch sind. Hinter solchen Algorithmen steckt meistens eine mathematische Operation, die in einer Richtung sehr einfach, in der anderen Richtung aber extrem schwierig ist. Es ist sehr einfach, zwei lange Zahlen zu multiplizieren, aber extrem schwierig, eine lange Zahl in ihre Primfaktoren zu zerlegen. Die Mathematiker suchen seit mehreren Jahrhunderten nach einem effizienten Algorithmus. Bis heute ohne durchschlagenden Erfolg.

Hartz: Da es sich bei dieser Verschlüsselung um eine echte Ende-zu-Ende-Verschlüsselung, also zwischen den jeweiligen Rechnern der Anwender, handelt, ist die Verschlüsselung hervorragend für Privatleute und für Einzelpersonen geeignet. In einer komplexen Unternehmensstruktur darf sie natürlich nicht eigenmächtig durch Mitarbeiter installiert werden, da damit IT Sicherheitsrichtlinien, wie zum Beispiel die interne E-Mail Archivierung, unterlaufen würden.

Wird auf diesen Umstand bei der Installation hingewiesen?

Herfert: Das Thema der Mail-Archivierung ist in der Tat schwierig. Das liegt daran, dass die entsprechenden Programme nicht auf Schlüssel eingestellt sind. Selbst die Hotlines der Hersteller sind hier oft überfragt – ein Indiz, dass solche Anfragen selten sind. Das liegt natürlich daran, dass es zu wenig Nutzer mit Schlüsseln gibt. Wir erwarten, dass sich dies ändert, wenn mehr Schlüssel verteilt sind. Bis dahin besteht ein sehr sinnvoller Workaround darin, dass die Firma eine Kopie des privaten Schlüssels anfertigt, um Nachrichten anstelle des Mitarbeiters entschlüsseln zu können. Das ist immer eine empfehlenswerte Strategie, auch ohne das Problem der Mail-archivierung. Der Zugriff auf diesen Schlüssel sollte durch organisatorische Regelungen präzise geregelt werden, um einen Missbrauch zu verhindern. Ein solches Vorgehen ist üblich und in meinen Augen im Businessbereich auch erforderlich.

Hartz: Derzeit muss der Antrag für ein Zertifikat persönlich gestellt werden. Die Person muss sich ausweisen. Auf diese Art ist die Möglichkeit, sich mal eben für ein Zertifikat zu registrieren, sehr eingeschränkt.

Welche Möglichkeiten wird es in Zukunft geben, schnell und einfach an ein Zertifikat zu kommen?

Herfert: Im Businessbereich bieten wir heute schon eine Identifizierung über eine Videokonferenz an. Dabei hält der Teilnehmer seinen Personalausweis in verschiedenen Winkeln in die Kamera, damit wir die Sicherheitsmerkmale überprüfen können. Das ist mit fast jedem Handy oder Tablet, den meisten Notebooks und den meisten externen Kameras möglich. Wir haben zudem Banken unter den Kunden, die das Recht haben, eigenständig Identifizierungen vorzunehmen. Auch Rechtsanwälte und Steuerberater können dieses Recht kostenfrei erhalten. In Kürze werden wir auch Post-Ident anbieten, sodass wirklich jeder die Möglichkeit hat, Verschlüsselungszertifikate zu erhalten.

Hartz: Mit welchen Browsern und Mailprogrammen kann ich die Zertifikate problemlos verwenden? Gibt es Einschränkungen bei aktuellen Browsern und Mailprogrammen?

Herfert: Wir unterstützen Outlook, Thunderbird, Firefox, den Internet Explorer und Google Chrome. Dabei gibt es keine Einschränkungen.

Hartz: Auf welchen Systemen funktioniert die einfache, automatisierte Installation des Zertifikates derzeit?

Herfert: Wir haben mit Microsoft Windows begonnen, weil dies das Betriebssystem ist, welches die überwältigende Mehrheit der Nutzer verwendet. Wir planen Versionen für iOS und Android, danach auch für macOS und Linux. Zurzeit kann ich aber noch keinen belastbaren Fertigstellungstermin nennen.

Wer einmalig Zugriff auf ein Windows-System hat, etwa in einer virtuellen Maschine, um seine Schlüssel zu erzeugen, kann diese ▸

exportieren, um sie dann unter macOS oder Linux zu nutzen. Das ist durch die Nutzung internationaler Standards möglich, erfüllt aber nicht unseren Anspruch an Benutzungsfreundlichkeit. Wir empfehlen diese Möglichkeit daher den Experten.

Hartz: Kann man die Zertifikate auch auf mobilen Endgeräten installieren und nutzen?

Herfert: Für iOS ist dies durch ein spezielles Export-Format der Schlüssel, das von der Volksverschlüsselungs-App bereitgestellt wird, möglich. Auch dazu ist Handarbeit erforderlich, wie eben beschrieben. Wir haben das Vorgehen in Schritt-für-Schritt-Anleitungen dokumentiert. Den Anspruch an maximale Einfachheit wird aber erst die iOS- bzw. Android-Version der Volksverschlüsselungs-App erfüllen.

Hartz: Sind die vom Fraunhofer SIT ausgestellten Zertifikate mit den derzeitigen Standards voll kompatibel? Oder für die Tekkies: Welche Klasse oder Sicherheitsstufe erfüllen die vom Fraunhofer SIT ausgestellten Zertifikate? Für welche Zwecke können sie verwendet werden?

Herfert: Wir erstellen S/MIME-Zertifikate der Klasse 3, die für fortgeschrittene elektronische Signaturen benutzt werden können. Dabei weist Klasse 3 auf die persönliche Identifizierung hin, also die Ausweiskontrolle im Face2Face-Kontext. Die Signaturen sind fortgeschritten, aber nicht qualifiziert. Qualifizierte elektronische Signaturen sind manuellen Signaturen gleichgestellt. Entsprechende Zertifikate sind aber sehr teuer und haben sich bis heute, 22 Jahre nach Einführung des ersten Signaturgesetzes in Deutschland, nicht flächendeckend durchgesetzt. Meiner Meinung nach werden sie es auch nie tun. Fortgeschrittene Signaturen sind aber keineswegs wertlos, sie ersetzen nur nicht automatisch die manuelle Signatur. Insbesondere Prozesse in Firmen lassen sich mit ihnen sehr gut abbilden, sogar so, dass auch sehr strenge Revisionsabteilungen ihr Einverständnis geben.

Insgesamt kann man die Zertifikate für drei Zwecke verwenden: Zum Signieren, zum Verschlüsseln und für die Authentifizierung. Der letzte Punkt bietet noch ein unglaubliches Potenzial, denn er bedeutet, dass die Zertifikate im Browser genutzt werden können, um dort webbasierte Log-Ins mit Passwörtern abzulösen. Die Konfiguration eines Web-Servers zur Umstellung von Passwörtern auf kryptografische Schlüssel ist in den meisten Fällen sehr einfach, da die wichtigsten Server darauf vorbereitet sind. Für den Nutzer ergibt sich ein Gewinn an Sicherheit und gleichzeitig eine Vereinfachung der Benutzung, denn er muss keine neuen Passwörter setzen, keine verwalten und auch keine Passwörter unter seinen Geräten synchronisieren. Eine derartig erfreuliche Koinzidenz ist sehr selten im Bereich der IT-Sicherheit.

Hartz: Sichere Zertifikate müssen von einem Trust Center ausgegeben werden, damit diese als »vertrauenswürdig« akzeptiert sind. **Welches Trust Center stellt die Fraunhofer-Zertifikate aus?**

Und wie wird deren Sicherheit gewährleistet?

Herfert: Wir haben unser eigenes Trustcenter aufgebaut und alle dazu notwendigen Maßnahmen ergriffen sowie die erforderlichen Dokumente verfasst. Das hatte den Vorteil, dass wir von niemandem abhängig waren und alle Schritte des Prozesses selber in der Hand hatten. Unser gesamtes Institut beschäftigt sich mit dem Thema IT-Sicherheit. Wir wissen sehr genau, wie ein solches System technisch und organisatorisch abzusichern ist.

Nachteilig für den Nutzer ist, dass unser Trustcenter vertrauenswürdig ist, aber nicht zu den im Betriebssystem vorinstallierten gehört. Bei der Installation der App erscheint eine Warnmeldung des Betriebssystems, die sich aus verständlichen Gründen nicht abschalten lässt. Wir arbeiten gerade an einer Kooperation mit einem Hersteller vorinstallierter Zertifikate. Noch in diesem Jahr wird die Warnmeldung dann verschwinden.

Hartz: Welche Ziele haben Sie sich mit der »Volksverschlüsselung« gesetzt? Wie viele Zertifikate wollen Sie unter das Volk bringen?

Herfert: Eine Zahl kann ich gar nicht nennen, aber die Möglichkeiten, Zertifikate zu nutzen, sollten sich verbessern. Mein Traum ist es, die Volksverschlüsselung in die Einwohnermeldeämter zu bringen. Dort gehört sie hin. Wir unterstützen gerne jedes Einwohnermeldeamt. Der Aufwand dort ist minimal.

Hartz: Herr Herfert, wir bedanken uns für das Interview und die Unterstützung in der Kooperation zwischen dem Fraunhofer-Institut für Sichere Informationstechnologie und dem BvD.

Der BvD hat seit April 2019 mit dem Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt, geleitet von Prof. Michael Waidner, eine Kooperation begründet. In gegenseitiger Zusammenarbeit wollen wir das Projekt »Volksverschlüsselung« weiter voranbringen und unseren Mitgliedern die Mailverschlüsselung auch in anderen Projekten wie zum Beispiel »Datenschutz geht zur Schule« vermitteln.

Das Fraunhofer-Institut hat beim Verbandstag im Juni in Berlin bereits vielen Mitgliedern ein kostenloses privates Zertifikat oder ein Zertifikat zur geschäftlichen Nutzung ausstellen können.

Das Zertifikat zur privaten Nutzung ist kostenfrei. Ein Zertifikat zur geschäftlichen Nutzung kostet 50 € jährlich.

Die nächste Möglichkeit für Mitglieder und Teilnehmer der direkten Registrierung und Ausstellung eines Zertifikates ist bei der Herbsttagung vom 23. bis 25. Oktober 2019 in Nürnberg.

Das Interview führte Jürgen Hartz, stellvertretender Vorstandsvorsitzender BvD, mit Michael Herfert, Abteilungsleiter Cloud Computing, Identity & Privacy am Fraunhofer-Institut für Sichere Informationstechnologie, Darmstadt.

Anzeige

Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE SIT

KEY2B

EINFACH E-MAILS VERSCHLÜSSELN UND DOKUMENTE SIGNIEREN

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Oliver Küch
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-213
Fax 06151 869-224
oliver.kuech@sit.fraunhofer.de

Worum geht's?
- E-Mail-Verschlüsselung
- Digitale Unterschriften
- Verbesserung und Absicherung von Geschäftsprozessen

Ohne E-Mail und IT geht heute in den meisten Unternehmen nichts mehr, doch die zunehmende Digitalisierung ist nicht ohne Risiko: Die Gefahren durch IT-basierte Angriffe, Computerkriminalität und Wirtschaftsspionage steigen und mit ihnen die gesetzlichen Anforderungen an IT-Sicherheit und Datenschutz. Verschlüsselung ist eine wirksame Möglichkeit die eigene Kommunikation zu schützen, doch entsprechende Lösungen eigneten sich bisher nur für IT-Experten und große Unternehmen. Mit Key2B gibt es jetzt erstmals eine professionelle Verschlüsselung für kleine und mittlere Betriebe. Sie eignet sich auch für Computernutzer ohne Fachkenntnisse und Betriebe ohne IT-Abteilung. Technologie und Verfahren sind bereits bei tausenden Nutzern erfolgreich im Einsatz.

Mit Key2B-Schlüsseln können Unternehmen gesetzliche Vorgaben einfach erfüllen und gleichzeitig ihre Betriebsabläufe verbessern. Nutzer können verschlüsselte und/oder signierte E-Mails versenden und empfangen – auch mit mobilen Geräten. Zusätzlich lassen sich Dokumente mit Standardsoftware elektronisch unterschreiben und archivieren. So können Unternehmen zum Beispiel interne und externe Prozesse wie Urlaubsanträge, Zeiterfassung, Auftragsänderungen oder Freigabeprozesse digital abbilden. Zusätzlich können Benutzer sich in geeigneten Web-Anwendungen sicher einloggen – ganz ohne komplizierte Passwörter.

Was ist Key2B?
- Laientaugliche Software zur Schlüsselerzeugung und Installation

Für wen eignet sich Key2B?
- Freiberufler
- Kleine und mittelgroße Unternehmen

Vorteile:
- Erfüllung von Datenschutz- und Compliance-Anforderungen dank standardkonformer S/MIME-Zertifikate
- Beschleunigung von Betriebsabläufen
- Digitale Signatur für Rechnungen und andere Dokumente

Was unterscheidet Key2B von anderen?
- Höchste Sicherheitsstufe durch Identitätsprüfung
- Echte Ende-zu-Ende-Verschlüsselung: Nur Absender und Empfänger sehen den Inhalt der E-Mails
- Usability by Design - Laientauglichkeit
- Einfache Integration: Nutzung bestehender E-Mail-Infrastruktur
- Zertifikate made in Germany

Systemvoraussetzungen:
- Betriebssysteme: Windows, macOS*, iOS*
- Mail-Clients: Outlook, Thunderbird, Apple-Mail*, Lotus Notes
- Webbrowser: Internet Explorer, Edge, Firefox, Chrome, Safari*

* Schlüssel müssen zurzeit noch auf einem Windows-Gerät erzeugt werden.Sie können dann exportiert werden, um sie auf Apple-Geräten zu nutzen.

DATENSCHUTZPRAXIS

ARBEIT 4.0 – DIE DIGITALISIERUNG DER ARBEITSWELT

Regina Mühlich

Die Datenschutz-Grundverordnung ist grundsätzlich technikneutral. Sie schreibt dennoch Prinzipien wie Privacy by Design und by Default verbindlich vor. Diese gelten u. a. für durch Beschäftigte genutzte Notebooks und Smartphones sowie für Apps, Tools und Software.

Es geht um »Digitalisierung der Arbeitswelt« und »Arbeit 4.0«. Schlagwörter, die Datenschutzbeauftragte, den Gesetzgeber, Unternehmen sowie Führungskräfte und Arbeitnehmer beschäftigen. Es entstehen neue Beschäftigungsformen, beschleunigte Kommunikation und flexiblere Prozesse.

Datenschutz ist Grundrechtsschutz[1]

In den letzten Jahren rückte der Datenschutz im Beschäftigtenverhältnis immer mehr und mehr in den Mittelpunkt. Im Beschäftigtenverhältnis ist es unvermeidlich, dass der Arbeitgeber personenbezogene Daten seiner Arbeitnehmer verarbeitet, an Auftragsverarbeiter und an Dritte weiterleitet. Dies geschieht u. a. um Gehälter und Sozialversicherungsbeiträge zu zahlen die Nutzung von Zeiterfassungssystemen sowie zur Kontrolle der Leistung und des Verhaltens der Mitarbeiter. Darüber hinaus geht es um einen ordnungsgemäßen und effizienten Betriebsablauf sowie um die Kommunikation innerhalb des Betriebes, mit Dienstleistern, verbundenen Unternehmen und Kunden.

Die technischen Entwicklungen eröffnen den Unternehmen, aber auch den Beschäftigten, viele Möglichkeiten, um Arbeit effizienter und effektiver zu gestalten. Die Risiken für die Persönlichkeitsrechte der Beschäftigten sind dadurch aber auch stark gestiegen und damit auch die Notwendigkeit, einen entsprechenden und wirksamen Schutz zu gewährleisten. Der Eintritt in die Welt der »Industrie 4.0« hebt diese Entwicklungen auf eine neue Stufe[2].

Was schützt das Datenschutzgesetz?

»Personenbezogene Daten« sind zentraler Begriff und Schutzgegenstand der Datenschutzrechte (u. a. DSGVO, BDSG). Gemäß Artikel 4 Nr. 1 DSGVO handelt es sich dabei um »alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (»betroffene Person«) beziehen, als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.«

Verbotsgesetz mit Erlaubnistatbestand

Wie bereits die »alten gesetzlichen Grundlagen« ist auch die Datenschutz-Grundverordnung ein Verbotsgesetz. Die Erlaubnistatbestände sind gleichranging und gleichwertig zu betrachten. Das bedeutet, der Umgang mit personenbezogenen Daten ist nur gestattet, wenn gemäß Artikel 6 DSGVO die »Rechtmäßigkeit der Verarbeitung«, eine von sechs Bedingungen (Art. 6 Abs. 1 lit. a – f DSGVO), erfüllt ist.

In Deutschland regelt das Bundesdatenschutzgesetz (BDSG), Abschnitt 2 Besondere Verarbeitungssituationen näher.

[1] Ehmann/Selmayr/Zerdick DS-GVO Art. 1 Rn 7f

[2] Arnold/Günther Arbeitsrecht 4.0, Kap. 6, A, Rn. 1

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

§ 26 BDSG regelt die Rechtmäßigkeit der Datenverarbeitung im Rahmen eines Beschäftigungsverhältnisses. In Abs. 1 heißt es »Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung […] erforderlich ist.«

Der Begriff »Beschäftigte« ist weit gefasst, darunter sind Bewerber, Aushilfe, Leiharbeiter, Auszubildende, Teilzeitkräfte, Praktikanten, Werkstudenten, ehemalige Beschäftigte usw. sowie auch »normale« Arbeitnehmer zu verstehen (§ 26 Abs. 8 BDSG).

Die Datenschutzgrundverordnung ist grundsätzlich technikneutral. Dennoch enthält sie ein paar Regelungen, die auch, oder vor allem, im Rahmen der neuen Arbeitswelt immer mehr an Bedeutung gewinnen.

Privacy by Design & Privacy by Default

Die DSGVO schreibt Prinzipien wie Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen verbindlich vor (Art. 25 DSGVO, ErwG 78).

Diese gelten u. a. für Notebooks und Smartphones der Beschäftigten, Apps, die Mitarbeiter nutzen, Smart Factory und vieles mehr.

Das existierende Grundprinzip im Datenschutzrecht lautet: Personenbezogene Daten dürfen nicht verarbeitet werden, es sei denn, es liegt eine Einwilligung vor oder eine gesetzliche Vorschrift gestattet den Datenumgang. Einem Gerätehersteller ist beispielsweise gesetzlich gestattet, jene personenbezogenen Daten des Kunden zu verarbeiten, die für die richtige Durchführung des Kaufvertrages oder aber für die Erbringung von Dienstleistungen notwendig sind.

Die geregelten Konzepte des Datenschutzes durch Technikgestaltung (»Privacy by Design«) und datenschutzfreundliche Voreinstellungen (»Privacy by Default«) sind nicht neu. Bereits in den 90er Jahren wurden sie von der Informationsfreiheits- und Datenschutzbeauftragten Ann Cavoukian (Ontario/Kanada) aufgegriffen, um das Risikopotenzial von Datenverarbeitungssystemen und -prozessen mittels proaktiver technischer Gestaltung zu vermindern.

Ein effektiver Datenschutz kann nicht nur durch eine reaktive ex-post Betrachtung eines Verarbeitungsvorgangs realisiert werden. Die Einhaltung der Anforderungen der DSGVO sind nur dann möglich, wenn technische Prozesse ex-ante, also im Vorhinein, mit dem Datenschutz in Einklang gebracht werden. Art. 25 DSGVO ist eine reine Verfahrensvorschrift und keine Voraussetzung für die Rechtmäßigkeit einer Verarbeitung i.S. Art. 5 ff DSGVO (ein so genannter Erlaubnistatbestand).[3]

Bewerbermanagement und Bewerberportale

Der Bewerbungsprozess ist als vorvertragliches Vertrauensverhältnis zu sehen. § 26 Abs. 1 BDSG besagt, dass personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses verarbeitet werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses […] erforderlich ist. Zu diesen Daten gehören im Bewerbungsverfahren beispielsweise Name und Anschrift, Telefonnummer und E-Mail-Adresse, Zeugnisse und Lebenslauf. Neben diesen typischen Bewerbungsunterlagen ist auch eine Speicherung von personenbezogenen Daten, die mit zulässigen Fragen erhoben werden, aus Datenschutzsicht unproblematisch.

Viele Unternehmen bieten Bewerbern die Möglichkeit, sich über ein spezielles Portal, also online auf der Unternehmenswebseite, zu bewerben. Dazu gehören Angaben zur Person und dem beruflichen Werdegang ebenso wie das Hochladen von Dokumenten wie Lebenslauf, Zeugnisse, Zertifikate, etc. Besonders in großen Unternehmen steuern solche E-Recruiting-Systeme den Ablauf eines Bewerbungsverfahrens und sind ressourcenschonend für den Personalbereich.

Wenn diese Bewerberportale rein als zusätzlicher Kommunikationskanal dienen, ergeben ▸

[3] Regina Mühlich, Datenschutzmanagement nach DSGVO - Privacy by Design & Privacy bei Default https://www.adorgasolutions.de/wp-admin/post.php?post=1957&action=edit

sich keine datenschutzrechtlichen Besonderheiten – Privacy by Design und by Default wie auch die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO sind selbstverständlich sicherzustellen. Umfasst die Bewerberseite z. B. einen Online-Fragebogen, muss der Arbeitgeber darauf achten, dass nur die für die Stellenbesetzung erforderlichen Angaben und die Grenzen des Fragerechts des Arbeitgebers eingehalten werden.[4]

Bewerbungsgespräche via Video

Immer beliebter, da auch zeit- und kostensparend, sind Bewerbungsgespräche mit videobasierten Diensten wie Skype oder Facetime. Die Aufzeichnung eines solchen Gespräches, bei dem der Arbeitgeber die Möglichkeit hat, das Verhalten, die Gestik und Mimik des Bewerbers mehrmals zu sehen und somit auch zu analysieren, bedarf einer genaueren datenschutzrechtlichen Betrachtung.

Zuerst gilt es eine Rechtsgrundlage für die Verarbeitung der Videodaten von Bewerbern zu finden. Die Einwilligung scheidet dabei grundsätzlich als Legitimation aus, wenn der potentielle Arbeitgeber zum Videointerview einlädt. Eine Einwilligung hat grundsätzlich freiwillig (selbstbestimmt und informiert) zu erfolgen. Dies wird für den Bewerber regelmäßig nicht gegeben sein, da er, sofern er die Teilnahme an dem Videogespräch ablehnt, davon ausgehen muss, dass seine Chancen im Auswahlverfahren gemindert werden.

Es versteht sich von selbst, dass die Nutzung von Software, die die Aufzeichnung mit Hilfe einer automatischen Bild- und/oder Sprachanalyse unterzieht, um Rückschlüsse auf die Persönlichkeit des Bewerbers zu ziehen, eine Grenze überschreitet und datenschutzrechtliche wie auch ethnische Bedenken aufwirft.

Fazit

Die Digitalisierung der Arbeitswelt, Arbeit 4.0, bringt viele Entwicklungen und Vorteile. Sie birgt aus Datenschutzsicht aber auch die Möglichkeit des Missbrauchs. Eine große Gefahr dabei ist u. a. die Profilerstellung und die automatisierte Entscheidung.

Andererseits können Zugriffe und Berechtigungen relativ einfach vergeben und monitort werden. Arbeitsabläufe in Unternehmen, vor allem im Personalbereich, werden vereinfacht, effizienter und effektiver gestaltet.

Unabhängig davon sind Art. 25 DSGVO Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen sowie Art. 32 DSGVO Sicherheit der Verarbeitung (technische und organisatorische Maßnahmen) und nicht zuletzt Art. 5 Abs. 2 DSGVO sicherzustellen.

Über die Autorin

Regina Mühlich
Geschäftsführerin der Managementberatung AdOrga Solutions GmbH

Als Expertin für Datenschutz, Datenschutz-Auditorin sowie Compliance Officer unterstützt sie mit ihrem Team Unternehmen im Bereich Datenschutz, Compliance und Qualitätsmanagement in Deutschland, Österreich sowie der Schweiz. Sie ist Lehrbeauftragte an der Hochschule Furtwangen, Mitglied des IDG-Expertennetzwerkes und Vorstandsmitglied des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

▶ consulting@AdOrgaSolutions.de

▶ www.AdOrgaSolutions.de

[4] Vgl. Sörup/Marquardt ArbRAktuell 2016, 103 (105)

CALIFORNIA CONSUMER PRIVACY ACT – EIN NEUES DATENSCHUTZNIVEAU FÜR DIE USA? ODER GAR EINE «MINI-DSGVO»?

Jutta Sonja Oberlin

I. Einleitung

2018 war ein grosses Jahr für den Datenschutz.

Die Mutter aller Datenschutzgesetze wurde am 25.05.2018 anwendbar: Die Datenschutz-Grundverordnung (DSGVO). Mit ihren weitreichenden und komplexen Datenschutzanforderungen und dem Potenzial für enorme Bußgelder, mit bis zu 4% des weltweiten Umsatzes, setzt diese ganz neue Massstäbe für den Datenschutz in Europa.

Während sich viele Unternehmen auf die Umsetzung der DSGVO konzentrieren, ist es besonders für global agierende Unternehmen wichtig, auch andere neue Datenschutzbestimmungen im Auge zu behalten, um Last-Minute-Arbeiten für die Einhaltung anderer internationaler Bestimmungen zu vermeiden.

Welche Gesetze müssen nun Unternehmen beachten, welche in Kalifornien tätig sind bzw. Daten von in Kalifornien ansässigen Personen verarbeiten?

In den USA gibt es kein einheitliches Bundesgesetz, welches den Datenschutz regelt. Die USA regelt den Datenschutz in verschiedenen Gesetzen, Bereichen und Bundesstaaten.

Schon 1972 hatten kalifornische Wähler beschlossen, das Recht auf den Schutz der eigenen Daten in die Verfassung zu inkludieren. Diese Ergänzung (sog. Amendment) etabliert für jeden kalifornischen Bürger ein durchsetzbares Recht auf Datenschutz inklusive dem Recht die eigenen Daten kontrollieren zu können bzw. eine Kontrolle über die gewerbliche Nutzung der eigenen Daten durch Dritte zu haben.

Seither hat Kalifornien diverse Massnahmen getroffen, um die Rechte der Bürger zu stärken. Beispielsweise wurden weitere Gesetze wie der Online Privacy Protection Act, The Privacy Rights for California Minors in the Digital World Act und «Shine the Light»[1] - ein kalifornisches Recht, welches den Datensubjekten das Recht gewährleistet zu erfahren, welche personenbezogenen Daten von Dritten über diese bearbeitet werden[2] - beschlossen. ▶

[1] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV

[2] https://www.pbwt.com/content/uploads/2018/06/California-Consumer-Privacy-Act1.pdf.

Beachtlich ist hierbei nicht nur die Fülle an fortschrittlichen Datenschutzgesetzen, sondern auch der Fakt, dass Kalifornien einer der einflussreichsten Entwicklungsstandorte im Bereich der Technik und Digitalisierung ist. Durch diese enorme Wirtschaftskraft im Technologiebereich ist gerade Kalifornien von datenverarbeitenden Technologien besonders betroffen. Genau aus diesem Grund müssen auch die Gesetze diesen technischen Entwicklungen standhalten können.

Ab 1. Januar 2020 soll zudem eine weitere bundesstaatliche Bestimmung in Kraft treten, welche Unternehmen im Anwendungsbereich beachten müssen: Das neuen kalifornische Datenschutzgesetz.[3]

Dieser Artikel soll einen Überblick über das kalifornische Verbraucherschutzgesetz geben, die Hauptmerkmale aufzeigen und die Unterschiede zur DSGVO evaluieren.

II. Was bisher geschah…

Der Act wurde zügig eingeführt und unterzeichnet, um zu verhindern, dass die Wähler bei den Wahlen im November einer ähnlichen Wahlinitiative gegenüberstehen.

Am 28. Juni 2018 unterzeichnete Gouverneur Brown den Assembly Bill 375, der heute als California Consumer Privacy Act (CCPA) von 2018 bekannt ist und den Verbrauchern neue Rechte in Bezug auf die Bearbeitung ihrer persönlichen Daten einräumt. Die kalifornische Generalstaatsanwaltschaft wird Vorschriften erlassen und eine breite Beteiligung der Öffentlichkeit anstreben, um die Ziele der CCPA zu fördern. Die Vorschriften zielen darauf ab, Verfahren zur Erleichterung der Verbraucherrechte im Rahmen des CCPA festzulegen und den Unternehmen Anleitungen zur Einhaltung zu geben.

Einer der Gründe für die Regulierung der Privatsphäre der Bürger von Kalifornien war der Datenschutzverstoss im März 2018, bei welchem ein Data-Mining-Unternehmen namens Cambridge Analytica Millionen von personenbezogenen Daten missbrauchte. In einer Reihe von Anhörungen im Kongress wurde darauf hingewiesen, dass personenbezogene Daten bei der Weitergabe im Internet möglicherweise missbräuchlich verwendet werden könnten. Infolgedessen kam aus der Bevölkerung verstärkt der Wunsch nach Datenschutzkontrollen und Transparenz auf.

Der CCPA gewährt den Verbrauchern[4] in der Tat vier Grundrechte in Bezug auf ihre persönlichen Daten.

Für die USA ist dies ein ganz neues Gebiet in Bezug auf den Datenschutz. Unternehmen werden in Kürze strengere Anforderungen erfüllen und ihr Geschäftsmodell möglicherweise umstrukturieren müssen.

III. Was soll durch die Revision bezweckt werden?

Die Revision soll den kalifornischen Datensubjekten, also den Konsumenten bei online und offline Geschäften[5] ihre Rechte bzgl. ihrer Daten wieder zurückgeben.

Darunter fällt einerseits die Kontrolle über die eigenen Daten und andererseits die geeigneten Schutzmassnahmen aus staatlicher bzw. gesetzlicher Perspektive.

In erster Linie geht es dabei um die Achtung von datenverarbeitenden Unternehmen, welcher betreffend die Verarbeitung von personenbezogenen Daten den Datensubjekten gewährleistet wird.

Diese Achtung umfasst hierbei sowohl die Transparenz bei der Datenverarbeitung, faire Geschäftspraktiken und die Gewährleistung der Rechte der Datensubjekte.

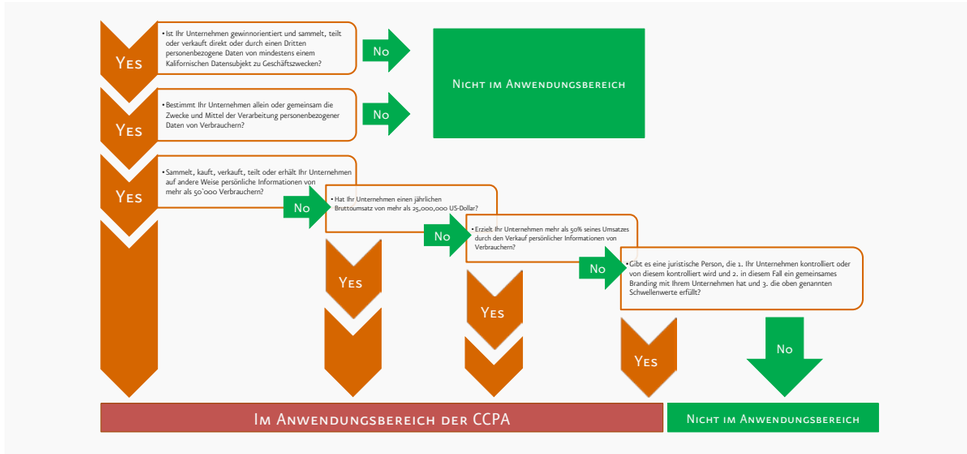
IV. Wichtige Legaldefinition des CCPA: Personenbezogene Daten

»Persönliche Information« werden wie folgt definiert:

»Information, die einen bestimmten Verbraucher oder Haushalt[6] identifiziert, sich auf diese/n bezieht, diese/n beschreibt, mit der Person in Verbindung gebracht werden kann oder vernünftigerweise direkt oder indirekt damit in Verbindung gebracht werden könnte.« Diese bietet eine nicht vollständige Liste von Beispielen, die einige ausführliche Beispiele enthält. Zu persönlichen Informationen gehören beispielsweise »kommerzielle Informationen« (einschließlich »Aufzeichnungen über persönliches Eigentum, gekaufte, erhaltene oder in Betracht gezogene Produkte oder Dienstleistungen oder andere Kauf- oder Verbrauchsgeschichten oder -tendenzen«), »Informationen über Internet- oder andere elektronische Netzwerkaktivitäten« (z. B. Browsing- und Suchhistorien), »Bildungsinformationen« und »Audio-, elektronische, visuelle oder ähnliche Informationen«.

V. Wer fällt unter den Anwendungsbereich der Norm?

Das Gesetz zielt auf gewinnorientierte Unternehmen[7], die in Kalifornien ansässige personenbezogene Daten erheben, verarbeiten und Geschäfte im US-Bundesstaat Kalifornien tätigen mit: (a) einem jährlichen Bruttoumsatz von mehr als 25 Mio. USD; oder (b) die persönlichen Informationen von 50.000 oder mehr Einwohnern, Haushalten oder Geräten in Kalifornien auf jährlicher Basis erhalten oder offen legen; oder (c) 50 Prozent oder mehr ihrer jährlichen Einnahmen aus dem Verkauf der persönlichen Daten von Einwohnern Kaliforniens ableiten. Das Gesetz hebt auch Konzernunternehmen solcher Unternehmen in den Anwendungsbereich, die ihre Marke teilen. Dies bedeutet, dass gemeinnützige Organisationen, kleine Unternehmen und / oder Unternehmen, die keine großen Mengen an persönlichen Informationen übermitteln und keine Marke mit einem verbundenen Unternehmen teilen, das unter das Gesetz fällt, vom CCPA ausgenommen sind.



V.1 Ausnahmen

Obwohl ein Unternehmen augenscheinlich unter das CCPA fallen könnte, gibt es eine Reihe von Ausnahmen, die die Anwendbarkeit des Gesetzes einschränken. Unter bestehende datenschutzrechtliche Bestimmungen fallende Unternehmen müssen zunächst feststellen, in welchem Umfang das CCPA für diese anwendbar ist.

GLBA-[8], CFIPA-[9] oder DDPA-[10] regulierte Unternehmen sind vom Klagerecht der Verbraucher betroffen, um gesetzlichen Schadenersatz zu verlangen.

HIPAA[11]-regulierte Unternehmen müssen die CCPA nicht einhalten, wenn sie ein Gesundheitsdienstleister, ein Gesundheitsplan oder eine Clearingstelle für das Gesundheitswesen sind, die in der gemäß der HIPAA festgelegten Datenschutz-, Sicherheits- und Verstossbenachrichtigung definiert sind.

CMIA[12]-regulierte Unternehmen müssen die CCPA nicht einhalten, wenn sie Gesundheitsdienstleister, Krankenversicherer und Einzelpersonen oder Unternehmen sind, mit denen sie Zugang zu medizinischen Informationen haben, einschließlich IT-Unternehmen (sogenannte Auftragnehmer).

Das Gesetz schließt zudem die Erhebung oder den Verkauf von persönlichen Informationen eines Verbrauchers aus dem Anwendungsbereich aus, wenn jeder Aspekt von diesem Geschäft

- vollständig außerhalb von Kalifornien stattfand,
- im Geschäftsprozess die Daten gesammelt wurden während der Verbraucher außerhalb Kaliforniens war,
- kein Teil des Verkaufsprozesses der personenbezogenen Daten in Kalifornien stattgefunden hatte
- und keine Daten verkauft wurden, als sich das Datensubjekt in Kalifornien aufhielt[13].

V.2 Anwendbar oder nicht? Vorgehen für möglich betroffene Unternehmen

Mithilfe einer Analyse können Unternehmen die Anwendbarkeit der CCPA auf ihr Unternehmen bestimmen. Beispielsweise muss ein Finanzinstitut, das bestehenden Datenschutzgesetzen wie dem GLBA unterliegt, wahrscheinlich die neuen Datenschutzrechte der CCPA für Kategorien oder bestimmte persönliche Informationen einhalten, die nicht bereits durch bestehende US-Datenschutzgesetze abgedeckt sind.

VI. Welche Rechte hat der Konsument unter dem CCPA?

Der Konsument hat in Bezug auf seine personenbezogenen Daten das vollumfängliche Recht der Transparenz und Datenübertragbarkeit.

VI.1 Die Transparenz soll gemäss SEC. 2. (i) Ziff. 1-5 CCPA durch folgende Garantien gesichert werden:

a) Ein Verbraucher hat das Recht zu verlangen, dass ein Unternehmen, welches personenbezogene Daten über den Verbraucher sammelt, diesem die folgenden Rechte gewährleistet: ▶

[3] California Consumer Privacy Act (CCPA)

[4] Natürlichen und in Kalifornien ansässigen Personen.

[5] 1798.175.

[6] Keine Legaldefinition im Gesetz.

[7] a. jede juristische Person oder gemeinnützige Organisation, welche in Kalifornien geschäftlich tätig ist (Unternehmenssitz ist nicht relevant)
b. Unternehmen, die von Datensubjekten personenbezogene Daten direkt oder indirekt durch einen Dritten (als Auftragsdatenverarbeiter) sammeln
c. Unternehmen die allein oder gemeinsam mit anderen die Zwecke die Verarbeitungszwecke dieser personenbezogenen Daten bestimmen (Joint Controller)

[8] The Gramm-Leach-Bliley Act.

[9] The California Financial Information Privacy Act.

[10] The Driver's Privacy Protection Act.

[11] The U.S. Health Insurance Portability and Accountability Act.

[12] The Confidentiality of Medical Information Act.

[13] 1798.145(a)(6).

(1) Mitteilung über die Kategorien personenbezogener Informationen, welche über das Datensubjekt gesammelt wurden.

(2) Mitteilung der Quellen, aus denen die persönlichen Daten gesammelt werden und mit welchen Dritten die Daten geteilt oder verkauft wurden.

(3) Das Recht der Datensubjekte den Verkauf ihrer personenbezogenen Daten zu verbieten.

(4) Das Recht der Datensubjekte Zugang zu den eigenen persönlichen Daten zu bekommen und ihr Recht auf Auskunft auszuüben.

(5) Das Recht der Datensubjekte auf eine Gleichberechtigung.

b) Transparenz ist zudem in Bezug auf den Verkauf von Daten gefordert. So muss die Unternehmung beim Verkauf folgende Informationen offenlegen[14],

(1) welche Daten gesammelt wurden,

(2) die Kategorien von Dritten, an die die personenbezogenen Daten verkauft wurden bzw. verkauft werden

(3) und für welchen geschäftlichen Zweck die Daten offengelegt wurden.

Eine Implementationsmassnahme bzgl. der Transparenz, wie genau mit den Daten der Datensubjekte umgegangen bzw. wie diese verarbeitet werden, ist die nun geforderte Datenschutzerklärung.

Inhalte und Anforderungen einer solchen Datenschutzerklärung sind die folgenden:

- Publikation auf Website oder anderweitig schriftlich
- Mind. einmal pro Jahr ein Update dieser Datenschutzerklärung
- Rechte der Datensubjekte gemäss des CCPA
- Information, wie eine Auskunftsanfrage zu machen ist
- Die Kategorien von personenbezogenen Daten, welche die Unternehmung über die Verbraucher die letzten 12 Monate in den verschiedenen Produktkategorien/Dienstleistungen bzw. Verarbeitungsprozesse sammelt
- Eine Liste, welche die Kategorien von Daten beschreibt, welche in den letzten 12 Monaten vom Unternehmen für geschäftliche Zwecke veröffentlicht oder verkauft wurden

[14] 1798.115.
[15] Auch: Datensubjekt.
[16] 1798.105.
[17] 1798.105.

VI.2 Verwirklichung der Datenübertragbarkeit durch den Gesetzgeber:

Ein Unternehmen, das personenbezogene Daten über einen Verbraucher sammelt, muss dem Verbraucher gemäß Absatz 3 von Unterabschnitt (a) von Abschnitt 1798.130 die angegebenen Informationen nach Eingang einer überprüfbaren Anfrage des Verbrauchers[15] offenlegen.

Ein Unternehmen, das personenbezogene Daten über Verbraucher sammelt, hat gemäß Absatz 5 Buchstabe b von Abschnitt 1798.130 Folgendes offenzulegen:

(1) Die Kategorien personenbezogener Informationen, die über diesen Verbraucher gesammelt wurden.

(2) Die Kategorien von Quellen, aus denen die persönlichen Daten gesammelt werden.

(3) Der geschäftliche oder kommerzielle Zweck zum Sammeln oder Verkaufen persönlicher Daten.

(4) Die Kategorien von Dritten, mit denen das Unternehmen personenbezogene Daten teilt.

(5) Die spezifischen persönlichen Informationen, die das Unternehmen über diesen Verbraucher gesammelt hat.

VI.3 Recht auf Vergessen[16]

Das CCPA statuiert, dass Datensubjekte das Recht haben, von einem Unternehmen die Löschung von deren personenbezogenen Daten zu fordern[17], welche dieses über den Verbraucher gesammelt hat.

Ausnahmen betreffend die Löschung der personenbezogenen Daten müssen jedoch berücksichtigt werden und personenbezogene Daten dürfen sodann trotz Löschanfrage weiterführend bearbeitet werden, wenn die folgenden Voraussetzungen erfüllt sind:

- Selbst erstellt wurden (z. B. ein Persönlichkeitsprofil aufgrund der Transaktionen und Einkäufe), oder
- Daten von Dritten stammen (z. B. Kundenberichte, Kundenverhalten usw.).

Weiteres zum Recht auf Vergessen in Punkt VII.6.

VI.4 Recht auf Opt-In für Kinder

Neue Anforderungen für den Austausch personenbezogener Daten für Kinder unter 16 Jahren werden zudem festgesetzt. Bei diesen wird das Alter gegenüber dem im Gesetz zum Schutz der Online-Privatsphäre für Kinder (»COPPA«) festgelegten, staatlich anerkannten Alter von 13 Jahren, auf 16 Jahre erhöht. Dies bedeutet, dass es Unternehmen untersagt ist, Informationen über Verbraucher zwischen 13 und 16 Jahren ohne die ausdrückliche Zustimmung der Vertreter/Datensubjekte zu verkaufen.

VII. Die DSGVO und das CCPA: Vergleichbar oder nur auf den ersten Augenschein ähnlich?

Im Folgenden werden einige der Hauptunterschiede und Ähnlichkeiten zwischen dem CCPA und der DSGVO vorgestellt.

VII.1 Anwendungsbereich

Der Anwendungsbereich der DSGVO erstreckt sich über die ganze EU, sowie auch im exterritorialen, also über die EU-Landesgrenzen hinaus.

Der Anwendungsbereich des CCPA bezieht sich auch auf Unternehmen, welche nicht ihren Sitz in Kalifornien haben. Jedoch wird hier nicht mit einem generalisierten Begriff des exterritorialen Anwendungsbereichs gearbeitet, sondern mit einer »abgespeckten« Version, welcher diese nur in Ausnahefällen vorsieht.

Dies bedeutet, dass Unternehmen, die personenbezogene Daten von in Kalifornien ansässigen Personen verarbeiten, dem Gesetz nicht unterliegen, es sei denn, sie erfüllen einen (oder mehrere) der folgenden Schwellenwerte: (i) Sie erzielen einen jährlichen Bruttoumsatz von 25 Mio. USD. (ii) sie haben die persönlichen Daten von 50.000 oder mehr Einwohnern, Haushalten oder Geräten in Kalifornien pro Jahr erhalten; oder (iii) sie haben 50 Prozent oder mehr ihres Jahresumsatzes mit dem Verkauf der persönlichen Daten von Einwohnern Kaliforniens erzielt.

VII.2 Die Rechte der Datensubjekte

In Bezug auf die Rechte, die dem Verbraucher gesetzlich gewährleistet werden, weisen die CCPA und die DSGVO bemerkenswerte Unterschiede auf. Die CCPA definiert im Gegensatz zur DSGVO keine rechtlichen Gründe für die Verarbeitung[18] und bedarf auch keiner ausdrücklichen Zustimmung. Das Gesetz zielt jedoch darauf ab die Rechte der Kalifornier auf deren Privatsphäre zu sichern, indem den Verbrauchern wirksame Möglichkeiten zur Kontrolle ihrer persönlichen Daten geboten werden. Dementsprechend hat nach dem CCPA der Verbraucher das Recht zu wissen, welche Kategorien von persönlichen Daten über sie gesammelt werden und gewährt diesen ein weitreichendes Recht auf Zugang zu Kopien dieser Daten. Obwohl diese Rechte denen der DSGVO ähneln, sieht die CCPA darüber hinaus bestimmte Verpflichtungen vor, beispielsweise die Verpflichtung, den Verbrauchern eine gebührenfreie Telefonnummer und eine Website-Adresse für die Übermittlung von Informationsanfragen zur Verfügung zu stellen.

VII.3 Weitergabe von personenbezogenen Daten zu kommerziellen Zwecken – Möglichkeit des Opt-Out bei Datenverkäufen

Eine weitere wichtige Bestimmung des CCPA, welche gemäß dieser Maßgabe in der DSGVO in dieser Form nicht zu finden ist, betrifft die Weitergabe personenbezogener Daten zu kommerziellen Zwecken. Die Weitergabe von personenbezogenen Daten in Bezug auf Einwohner Kaliforniens an Dritte ist als solche nicht verboten. Kalifornier haben jedoch das Recht, den Verkauf ihrer personenbezogenen Daten zu widerrufen.[19] Um dieses Recht zu stärken, müssen Unternehmen auf ihrer Homepage einen Link mit dem Titel »Meine persönlichen Daten nicht verkaufen« bereitstellen, über den der Verbraucher die Möglichkeit hat, sich abzumelden.[20]

Dieser Link muss zusammen mit einer Beschreibung des Rechts auf Opt-Out in die Datenschutzerklärung aufgenommen werden. Unter Berücksichtigung des allgemeineren Rechts der DSGVO, die Verarbeitung personenbezogener Daten einzuschränken oder zu beanstanden, könnte es für Unternehmen immer schwieriger werden, personenbezogene Daten zu verkaufen.

VII.4 Anti-Diskriminierung: Keine wirtschaftlichen Nachteile durch die Ausübung der Rechte der Datensubjekte

Es ist Unternehmen untersagt, Waren oder Dienstleistungen zu verweigern, unterschiedliche Preise zu berechnen oder den Verbrauchern, die ihre Persönlichkeitsrechte ausüben, eine schlechtere Qualität der Dienstleistungen zur Verfügung zu stellen.[21] Andererseits dürfen Unternehmen finanzielle Anreize für die Erhebung oder den Verkauf personenbezogener Daten bieten und sogar den Preis oder die Qualität von Waren und Dienstleistungen differenzieren, wenn dieser Unterschied in direktem Zusammenhang mit dem Wert steht, den die Daten für den Verbraucher darstellen. Da diese letzten Ausnahmen die Regel zu verdrängen scheinen, ist immer noch ungewiss, wie sich die zulässigen Preisunterschiede in der Praxis auswirken werden. Da die CCPA jedoch als in Arbeit befindlich angesehen wird, ist zu erwarten, dass diese Bestimmung Gegenstand künftiger Änderung ist.

VII.5 Meldung von Verletzungen des Schutzes personenbezogener Daten

Wenn es um Datensicherheit und Reaktion auf Datenschutzverletzungen geht, ist die CCPA tendenziell weniger streng ▸

[18] Art. 6 DSGVO.
[19] 1798.135(a)(5).
[20] 1798.120(a).
[21] 1798.125.

als die DSGVO[22]. Obwohl Unternehmen verpflichtet sind, angemessene Sicherheitsverfahren und -praktiken zu implementieren und aufrechtzuerhalten, welche der Kategorie der Daten entsprechen müssen, sind sie nicht verpflichtet die Datenschutzverletzungen zu melden, wenn diese auftreten.

Bei Datenschutzverstössen ist jedoch eine Zivilklage der Betroffenen möglich.[23]

VII.6 Recht auf Vergessen

Gemäss Art. 17 DSGVO räumt diese dem Datensubjekt das Recht ein, zu verlangen, dass ein für die Verarbeitung Verantwortlicher alle[24] betreffenden personenbezogenen Daten löscht.

Nun hat Kalifornien eine eigene Version dieses Rechts erlassen. Der relevante Teil der CCPA gewährt Verbrauchern das Recht, die Löschung ihrer persönlichen Daten zu beantragen. Nach einer kürzlich vorgenommenen Änderung muss dieses Recht den Verbrauchern nur in einer »angemessen zugänglichen Form« mitgeteilt werden. Vor dieser Änderung musste dieses Recht von den Unternehmen im Anwendungsbereich der Norm, in der Datenschutzrichtlinie veröffentlicht werden.

Das Recht auf Löschung im Rahmen der CCPA ist wie bei der DSGVO nicht unbegrenzt. Viele der Einschränkungen der DSGVO spiegeln sich im kalifornischen Recht wieder und enthalten Gründe, aus denen ein Unternehmen einen Löschungsantrag ablehnen kann.

Eine Löschung ist dann abzulehnen, wenn Folgendes zutrifft:

- Erforderlichkeit der Daten, um die Transaktion abzuschließen, für die sie abgeholt wurde oder für die Bereitstellung von Waren oder Dienstleistungen, die vom Verbraucher angefordert wurden
- Verwendung der Daten im Rahmen der Geschäftsbeziehung mit dem Verbraucher
- Erforderlichkeit zum Zwecke einer Vertragsausführung
- Zur Erkennung von Sicherheitsvorfällen und zum Schutz vor böswilligen, betrügerischen oder illegalen Aktivitäten
- Betreibung wissentschaftlicher, historischer oder statistischer Forschung im öffentlichen Interesse
- Verwendung ausschließlich für interne Zwecke, die den Erwartungen des Verbrauchers angemessen entsprechen
- Erforderlichkeit zur Einhaltung einer gesetzlichen Verpflichtung oder geltender Gesetze

Die CCPA enthält auch eine Ausnahmeregelung für Anträge, wenn sie ein Recht auf freie Meinungsäußerung beeinträchtigen, das Recht eines anderen Verbrauchers auf freie Meinungsäußerung gewährleisten oder ein anderes gesetzlich vorgesehenes Recht ausüben.

VII.7 Strafmass

Die Vollstreckung des CCPA liegt gemäss dem California Business & Professions Code § 17200 bei dem kalifornischen Generalstaatsanwalt[25], der eine Zivilklage gegen Unternehmen erheben kann[26], um Schadensersatz in Höhe von bis zu 7500 USD pro vorsätzlicher Datenschutzverletzung im Sinne des CCPA vorsieht.

Unbeabsichtigte Verstöße, die nicht innerhalb von 30 Tagen nach Benachrichtigung behoben werden, können zu Strafen mit bis zu 2500 USD pro Verstoß führen.

Nur im Falle eines Datendiebstahls oder einer Verletzung der Datensicherheit haben die Verbraucher selbst ein Recht auf eine private Klage auf gesetzlichen Schadenersatz zwischen 100 und 750 US-Dollar pro Verbraucher und Vorfall oder auf tatsächlichen Schadenersatz, je nachdem, welcher Betrag höher ist, sowie auf jede andere von einem Gericht für angemessen erachtete Entschädigung.[27]

VIII. Gemeinsam Verantwortliche (Joint Controller)

Gemäss Art. 26 DSGVO ist gemeinsam verantwortlich, wer mit einem anderen Verantwortlichen bzw. mit mehreren Verantwortlichen gemeinsam die Zwecke und Mittel der Datenverarbeitung festlegt.

Bei dem CCPA könnte eine Joint-Controller-ähnliche Beziehung vorliegen, wenn ein Unternehmen indirekt ein Geschäft im Rahmen des CCPA macht. Unternehmen, die von einem Unternehmen kontrolliert werden oder unter einer gemeinsamen Marke stehen, gelten indirekt als Unternehmen, sofern das Mutterunternehmen des Unternehmens selbst als Unternehmen im Rahmen der CCPA gilt. Dies würde die Anforderungen des CCPA auch auf indirekte Unternehmen ausweiten, die außerhalb Kaliforniens ansässig sind. Das indirekte Geschäft wird durch ein direktes Geschäft, eine gemeinsame Infrastruktur, die es beiden Arten von Unternehmen ermöglicht, ihre individuellen Interessen zu verfolgen, zu einem »Geschäft« nach dem Gesetz. Die CCPA dehnt die Verpflichtungen auf indirekte Unternehmen aus, sieht jedoch nicht ausdrücklich gesamtschuldnerische Verpflichtungen zwischen einem indirekten und einem direkten Unternehmen vor. Der kalifornische Generalstaatsanwalt hat zu diesem speziellen Thema noch keine Leitlinien vorgelegt.

IX. Fazit

Mit dem CCPA bricht eine neue Epoche des Datenschutzes in den USA an.

Neben den oben angesprochenen Unterschieden haben das CCPA und die DSGVO auch viel gemeinsam. Beide Gesetze befassen sich mit den gleichen Themen, wie bspw. der Transparenz und sehen jeweils ein ähnliches Recht auf Löschung personenbezogener Daten (»Recht auf Vergessen«) sowie ein Recht auf Datenübertragbarkeit vor.

Bestimmte CCPA-Anforderungen überschneiden sich mit den bestehenden DSGVO-Anforderungen für individuelle Rechte.

Auch wenn augenscheinlich das CCPA nur grössere Unternehmen in den Anwendungsbereich fasst, ist dies jedoch bei näherer Betrachtung nicht der Fall.

Aufgrund der weiten Eingrenzungen des Anwendungsbereiches können beispielsweise auch Restaurants, Cafés oder kleinere Online-Anbieter in den Anwendungsbereich der Norm fallen. Das Gesetz gilt für jede werbefinanzierte Website, die über ein Jahr verteilt 50.000 eindeutige IP-Adressen »erhält«.

Diese niedrige Schwelle lässt sogar die kleinsten werbefinanzierten Websites in den Anwendungsbereich fallen.

Unternehmen im Anwendungsbereich müssen sich bewusst sein, dass dieses Gesetz, besonders für kleinere bzw. nicht global agierende Unternehmen, welche die DSGVO nicht implementieren mussten, eine Mammutaufgabe darstellt und die Implementation Zeit und Budget in Anspruch nimmt.

So wird Unternehmen geraten sich einen vollumfänglichen Überblick über ihre Unternehmenslandschaft inkl. aller Datenverarbeitungsaktivitäten zu machen und mittels einer Lückenanalyse den Ist- und Soll Zustand zu beurteilen.

Nach dieser Beurteilung sollte eine realistische und risikobasierte Umsetzungsroadmap erstellt werden, welche die Umsetzung der einzelnen Anforderungen im Unternehmen gemäss internen Anforderungen und gesetzlichen Ansprüchen aufzeigt.

Über die Autoren

Jutta Sonja Oberlin

CIPP/E, CIPM, zertifizierte Datenschutzbeauftragte, zertifizierte Compliance Officer (Universität Augsburg), arbeitet als Unternehmensberaterin im Security Team der PWC in Zürich. Mit einer fundierter juristischen Grundausbildung an der Universität Zürich und einem Master in Compliance und Wirtschaftsrecht, sowie ihrer langjährigen Erfahrung bei der Beratung von Unternehmen in Bezug auf datenschutzrechtliche Themen aller Art, hat sie die besten Voraussetungen, um ihre Kunden praxisnah, unternehmensorientiert und nach den Best Practice Erfahrungen zu beraten. Ihre Expertise reicht von der DSGVO, BDSG, DSG bis hin zu internationalen Regulationen, wie das Chinesische Cyber Security Law, Datenschutz in den Staaten des mittleren Osten, USA und Russland.

[22] Art. 33 DSGVO.
[23] Siehe VII.7 Strafmass.
[24] Mit Ausnahmen.
[25] California Attorney General's office.
[26] 1798.155.
[27] 1798.150.

DATENSCHUTZPRAXIS/MEDIZIN

GESUNDER DATENSCHUTZ

Lothar Determann

Mit Methoden personalisierter Medizin können Ärzte wirksamer Diagnosen erstellen und Kranke heilen. Jeden Tag lernen wir von neuen Medikamenten, Medizingeräten und Heilmethoden, die mittels moderner Informationstechnologien entwickelt, verbessert oder eingeführt werden können.

Gleichzeitig werden Datenschutzregelungen immer restriktiver und behindern zunehmend den medizinischen und technischen Fortschritt in einem Maße, der mittlerweile ungesund ist. Ärzte, Forscher, Entwickler, Unternehmen, der Staat und andere Stellen müssen mehr Daten erheben, untersuchen und austauschen, nicht weniger. Statt Datenverarbeitungsverbote mit Erlaubnisvorbehalt, Datenminimierungsgebote oder bürokratische Hürden aufzustellen sollten sich Gesetzgeber auf konkrete Gefahren und Risiken konzentrieren. Wenn es z. B. darum gehen sollte mögliche Diskriminierung durch Arbeitgeber oder Versicherungsunternehmen zu verhindern, sollten Arbeits- oder Versicherungsgesetze angepasst werden, aber das ist kein Grund Datenverarbeitung allgemein zu verbieten oder einzuschränken. Eine Überdosis von Datenschutzregulierung wirkt giftig und kann mehr Patienten das Leben kosten als Krankenhauskeime.

I. Fortschritt in Medizin und Datenverarbeitung

Niedergelassene Ärzte, Krankenhäuser und Krankenkassen führen Patientenakten in elektronischer Form. Digitale Gesundheits-Apps begleiten uns in Echtzeit auf Schritt und Tritt. Immer mehr medizinische Geräte in Krankenhäusern und Arztpraxen werden in Netzwerke eingebunden und liefern massenweise Daten, die wiederum über KIS-Systeme (Klinikinformationssysteme) und Praxissoftware weiterverarbeitet und gespeichert werden. Mit der Einrichtung sog. Biobanken, Datenbanken biologischen oder genetischen Materials, wird die Grundlage zu digitaler Verarbeitung und potentiellem Austausch auch von genetischen Informationen geschaffen. Gleichzeitig verlagert sich im Rahmen der sog. Telemedizin der Behandlungsvorgang immer mehr in das digitale Umfeld, werden ärztliche Beratung und Behandlung online durchgeführt. Die Fülle an vorhandenen Daten bis in die genetische, Zusammensetzung' des Menschen hinein gibt der Medizin eine neue Grundlage zur Erforschung und Erprobung neuer Behandlungsoptionen. Unter den Schlagworten der personalisierten Medizin (im US-Sprachgebrauch auch als precision medicine bezeichnet) und Pharmakogenetik (als auf die genetischen Verhältnisse des Patienten abgestimmter Medikation) werden nach Lebensumständen, Umweltfaktoren und biologisch-genetischer Veranlagung des Patienten maßgeschneiderte Medikation und Behandlungsoptionen entwickelt.

All das macht die Medizin im 21. Jahrhundert datenintensiver. Die Erfassung von Gesundheitsdaten bietet Chancen für eine verbesserte Analyse von Krankheitsfaktoren, verbesserte Diagnose und Heilungschancen sowie für niedrigere Kosten und eine gesteigerte Effizienz im Gesundheitssystem. Die Verarbeitung der gesammelten Daten schafft aber gleichzeitig auch Risiken für die beteiligten Patienten, Ärzte und forschenden Mediziner. Diese Risiken reichen von Diskriminierung und Stigmatisierung auf Grundlage der erlangten Daten über unerwünschtes Wissen über die eigene Gesundheit bis zu betrügerischem oder erpresserischem Datenmissbrauch und fordern das geltende Rechtssystem heraus.

Der Umgang mit Gesundheitsdaten wird nach geltendem Recht durch Vorschriften des Datenschutzrechts sowie Regelungen über den Schutz der Privatsphäre und der ärztlichen Schweigepflicht reguliert. Das Gebiet des Datenschutzrechts hat in den vergangenen Jahren eine zunehmend strengere Regulierung erfahren, die Gefahren für eine zukünftige datenbasierte und präventive Medizin begründet. Außerdem ist die Beschaffung von vorbestehenden Patientendaten, die aus anderen Gesundheitseinrichtungen stammen, deutlich zeit- und arbeitsaufwändiger, wodurch es zu Verzögerungen im Behandlungsprozess kommt. Dabei verlangt der Schutz von Gesundheitsdaten aufgrund ihrer sensiblen Natur nach einem hohen Schutzniveau. Gleichzeitig verlangen die drei Teilbereiche der Medizin, namentlich die Behandlung von Krankheiten, deren Vorbeugung und die Weiterentwicklung der vorhandenen Instrumente zur Behandlung und Vorbeugung von Krankheiten zunehmend nach umfassender Datenverarbeitung.

II. Datenschutzrecht, Schutz der Privatsphäre und Patientengeheimnis

Die Verarbeitung von Gesundheitsdaten wird in Europa reguliert durch Vorschriften des Datenschutzrechts, in den USA durch Vorschriften zum Schutz der Privatsphäre (data privacy). Dazu treten Regelungen zum Schutz des Patientengeheimnisses. Dabei zeigt sich in Europa eine allgemein angelegte, restriktive Regulierung der Datenverarbeitung mit weitem Anwendungsbereich, während in den USA eine Vielzahl von bereichs- und gefahrenspezifischen Regelungen gelten.

1. In Europa

Beim Datenschutz geht es vornehmlich um den Schutz des Einzelnen (des »Betroffenen«) vor den Auswirkungen automatisierter Datenverarbeitung. In Europa ist das Datenschutzrecht mit Inkrafttreten der EU-Datenschutzgrundverordnung (Verordnung (EU) 2016/679 – DSGVO), der in allen EU-Mitgliedsstaaten unmittelbare Geltung zukommt, weitgehend harmonisiert. Nach europäischem Datenschutzrecht ist die automatisierte Datenverarbeitung grundsätzlich verboten. Unternehmen und andere Stellen dürfen personenbezogene Daten nicht verarbeiten, es sei denn, sie holen die Einwilligung des Betroffenen ein oder können einen anderen gesetzlich anerkannten Rechtfertigungsgrund geltend machen. Europäische Datenschutzgesetze sollen die automatisierte Verarbeitung personenbezogener Daten soweit wie möglich verhindern oder einschränken, sogar in Bezug auf öffentlich frei verfügbare Daten.

Für Gesundheitsdaten, im europäischen Recht (Art. 4 (15) DSGVO) definiert als »personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen« bestehen weitergehende Einschränkungen. Die Verarbeitung dieser Daten ist verboten, soweit nicht eine ausdrückliche Einwilligung des Betroffenen für einen oder mehrere festgelegte Zwecke vorliegt (Art. 9 DSGVO).

2. In den USA

Im Kontrast zur europäischen Regulierung ist in den USA die Datenverarbeitung grundsätzlich erlaubt. Gefahren für die Privatsphäre und die Vertraulichkeit der Kommunikation der Bürger wird durch einzelne Datenschutzgesetze begegnet, die auf die jeweilige Industrie und Gefahrenlage zugeschnitten sind (Determann 2016). So gelten für Gesundheitsdaten die Vorschriften des Health Insurance Portability and Accountability Act (HIPAA), der detaillierte technische und organisatorische Sicherheitsanforderungen verlangt sowie Belehrungspflichten und vereinzelt Einwilligungserfordernisse vorsieht. HIPAA wurde als Ausgleichsmaßnahme im Zusammenhang mit einem Gesetz zur Förderung elektronischer Übermittlung von Gesundheitsdaten zwischen Ärzten und Versicherungen erlassen. ▸

Unter HIPAA fallen Krankenhäuser, Anbieter von Gesundheitsdiensten sowie deren Abrechungsdienstleister. Die Auslagerung einer Datenverarbeitung an externe Dienstleister steht unter dem Vorbehalt der vertraglichen Verpflichtung zu umfangreichen Sicherheitsmaßnahmen. Auf bundesstaatlicher Ebene können daneben weitere Regelungen existieren. So hat beispielsweise der US-Bundesstaat Kalifornien in Form des Confidentiality of Medical Information Act auch Vorschriften für Onlinedienste erlassen.

3. Einwilligung oder Anonymisierung

Der Umgang mit Gesundheitsdaten in der heutigen Medizin basiert auf beiden Seiten des Atlantiks im Wesentlichen auf zwei Säulen: einer Einwilligung des Betroffenen oder der Anonymisierung von Daten. Diese Praxis wird durch die Beschaffung und Verarbeitung immer größerer Mengen an Gesundheitsdaten auf die Probe gestellt.

Dabei ist zu unterscheiden zwischen der Diagnose und Behandlung von Patienten und der Datenverwendung zu Forschungszwecken: Im Falle der medizinischen Behandlung und Versorgung eines konkreten Patienten, sei es im Wege der Telemedizin unter Nutzung von Fernkommunikationstechniken oder der »klassischen« Behandlung in der Praxis des niedergelassenen Arztes dürfte eine Anonymisierung von Gesundheitsdaten häufig nicht in Betracht kommen, um nicht die Anbindung an den zu behandelnden Patienten zu verlieren. Demgegenüber kann vor einer Datenverarbeitung in der medizinischen Forschung oder auch im Bereich der internen Revision von Gesundheitseinrichtungen zumindest theoretisch eine Anonymisierung von Daten erfolgen.

Der Vorgang der Anonymisierung von Daten stellt sich dabei aber praktisch als zunehmend unmöglich und vor allem kontraproduktiv heraus. Denn die unwiderrufliche Entfernung von Merkmalen aus Datensätzen, die eine Zuordnung zu einer bestimmten Person ermöglichen, ist praktisch schwer zu erreichen. Zudem braucht personalisierte Medizin personenbezogene Gesundheitsdaten.

4. Patientengeheimnis

Neben datenschutzrechtlichen Vorschriften sind Mediziner auch durch ärztliches Standesrecht zur Wahrung des Patientengeheimnisses verpflichtet. Dieses dient – ähnlich der datenschutzrechtlichen Vorschriften – dem Interesse des Einzelnen an der Geheimhaltung bestimmter (gesundheitsrelevanter) Tatsachen als Ausprägung des Rechts auf informationelle Selbstbestimmung. Zum anderen beruht die ärztliche Schweigepflicht aber auch auf Interessen des Gemeinwohls. Die Verpflichtung zur Verschwiegenheit dient dazu, das allgemeine Vertrauen im Arzt-Patienten-Verhältnis zu stärken, um so die Funktionsfähigkeit des Gesundheitssystems zu schützen.

III. Gefahren durch Datenverarbeitung

Patienten, Forscher und Ärzte sehen sich mit der zunehmenden Erhebung und Speicherung von Gesundheitsdaten neuen Risiken ausgesetzt. Die Erfassung und Zugänglichmachung von Gesundheitsdaten kann zu einer Stigmatisierung der Beteiligten führen: Patienten mit ansteckenden Krankheiten wie HIV oder tabuisierten Erkrankungen wie Depression können bei Aufdeckung ihrer Krankheit gesellschaftliche Ausgrenzung erfahren. Behandelnde Ärzte können durch die Einsichtnahme der Öffentlichkeit in ‚schlechte' Statistiken ebenso einen Reputationsschaden erleiden wie Forscher durch ‚falsche' Forschungsergebnisse. Versicherungen könnten auf Grundlage erhobener Gesundheitsdaten einzelne Kunden mit erhöhten Tarifen für Kranken-, Lebens- oder Berufsunfähigkeitsversicherungen belasten. Arbeitgeber könnten erhobene Gesundheitsinformationen zum Anlass nehmen, ihre Arbeitnehmer einer Leistungskontrolle zu unterziehen oder bei Bewerbern von einer Einstellung ganz abzusehen. Patienten sehen sich mit unerwünschtem Wissen über den eigenen Gesundheitszustand durch die Aufdeckung von genetischen Risiken oder vorhandener Erkrankungen konfrontiert, die ihre Lebensplanung auf den Kopf stellen können.

Die zur Datenverarbeitung notwendige Niederlegung von Gesundheitsinformationen macht diese auch angreifbar für kriminelle Aktivität. Unbefugte können sich Zugriff zu bei Krankenkassen, Ärzten oder Forschungseinrichtungen gespeicherten Daten verschaffen und die so ‚erbeuteten' Informationen zum Schaden der Betroffenen einsetzen. Patienten könnten mit dem Wissen über eine ‚anrüchige' Erkrankung erpresst werden. Die Kenntnis von Gesundheitsinformationen kann in den Händen Unbefugter Grundlage für Identitätsdiebstahl oder betrügerische Angebote wie vermeintliche Wunderheilmittel oder schlicht gefälschte Arzneimittel sein, die aus der erhöhten Verletzlichkeit eines ernsthaft Erkrankten Kapital zu schlagen versuchen.

IV. Gefahren durch Datenschutz

Die beschriebenen Risiken durch Datenverarbeitung dürfen nicht den Blick darauf verstellen, dass die geltenden Datenschutzregeln ihrerseits erhebliche Risiken verursachen, nämlich für die Zukunft der Medizin und damit für die Gesundheit, indem Datenschutz ungebührlich die Datenverarbeitung zugunsten von Menschen erschweren kann. Roland Eils, Gründungsdirektor des BIH-Zentrums für Digitale Gesundheit des Berlin Institute of Health und Professor an der Berliner Charité, beklagte kürzlich »dass ein überzogener Datenschutz jetzt und hier in Deutschland Leben gefährdet.«

1. Gesteigerter Datenbedarf in der Medizin

Die heutige Medizin braucht unabhängig davon, ob es sich um Fragen der Behandlung, Prävention oder medizinischen Forschung handelt, mehr Daten. Der Einsatz von Datenverarbeitung kommt dabei dem Patienten zugute: Röntgenbilder, die in einer elektronischen Gesundheitsakte hinterlegt sind, und so ohne großen Aufwand von Arzt zu Arzt weitergereicht werden können, liegen bei einem Arztwechsel bereits vor und müssen nicht erneut angefertigt werden. Behandelnde Ärzte können sich durch einen eröffneten Zugang zur gesamten Krankengeschichte eines Patienten ein besseres Bild von der Lage machen und ihre Behandlung auf den individuellen Patienten abstimmen. In der Forschung können durch Big Data Anwendungen zuvor nicht in Zusammenhang gebrachte Datensätze kombiniert und verknüpft werden. Ein gesteigerte Menge und Qualität von Gesundheitsdaten erhöht die Erfolgschancen einer solchen Forschung und kann bisher unbekannte Zusammenhänge aufdecken und so zu einem verbesserten Verständnis von Krankheitsursachen und Therapiechancen beitragen. Auch können so seltene aber relevante Nebenwirkungen von Medikamenten oder Therapien rascher erkannt werden. Werden Daten über medizinische Behandlungen erfasst, macht dies die Behandlungsvorgänge zum Wohle der Patienten transparenter. Fehler können leichter aufgedeckt oder ganz vermieden werden. Unter wirtschaftlichen Gesichtspunkten kann eine erhöhte Datenerfassung und verbesserte Verarbeitung zu einer gesteigerten Effizienz und damit Kostenersparnissen in den weltweit unter Kostensteigerungen leidenden Gesundheitssystemen führen und so Beitragszahler und öffentliche Kassen entlasten.

Das Datenschutzrecht läuft Gefahr diese Entwicklungen zu behindern, durch Erfordernisse informierter, freiwilliger, spezifischer und ausdrücklicher Einwilligung und in Europa zusätzlich durch das generelle Verbot automatisierter Verarbeitung personenbezogener Daten, das Datensparsamkeitsgebot, die Pflicht zur Löschung nicht mehr akut benötigter Daten und die aus diesen Ver- und Geboten folgende Notwendigkeit strenger Zweckbindung.

2. Verhinderung der Gefahrenabwehr

Die Verarbeitung von Daten kann auch zur Abwehr von Gefahren eingesetzt werden. Bereits heute dienen Big Data Anwendungen der öffentlichen Gesundheit. Die US-amerikanischen Centers for Disease Control and Prevention (CDC) verfolgen eine Strategie zur verbesserten Datenverarbeitung und Zusammenführung von Daten über mit Drogen im Zusammenhang stehende Todesfälle zur Eindämmung und Überwachung der grassierenden Opioid-Epidemie. Gesundheitsbehörden nutzen weltweit Mobilfunkdaten, um Bevölkerungsströme im Zuge von Epidemien oder Naturkatastrophen abzubilden und so eine mögliche Verbreitung von Krankheiten vorherzusehen und einzudämmen.

Auf einer individuelleren Ebene können Mediziner nach geltendem Recht verpflichtet sein, Informationen über den Gesundheitszustand eines Einzelnen zurückzuhalten, auch wenn ihre medizinische Einschätzung eine Gefährdung anderer Personen begründet. Eine Warnung von Angehörigen oder öffentlichen Stellen ist Ärzten auch im Fall der Feststellung einer ansteckenden Krankheit bei einem Patienten nicht ohne weiteres möglich, wenn sich der Patient entscheidet seine Erkrankung geheim zu halten und z.B. durch eine HIV-Infektion andere Personen gefährdet.

Eine allein auf den Einzelnen abstellende Einwilligungslösung im Datenschutzrecht verhindert eine effiziente Gefahrenabwehr. Gute Gründe sprechen dafür, Gesichtspunkte des öffentlichen Interesses und des Gemeinwohls stärker in den Vordergrund zu rücken.

V. Lösungsansätze

Die dargestellten Entwicklungen in der Medizin sollten Anlass geben, den Datenschutz im Bereich der Medizin des 21. Jahrhunderts neu auszurichten.

1. Datenverarbeitung selbst schadet Patienten nicht

Zunächst sollte das generelle Verbot der Verarbeitung personenbezogener Daten im europäischen Datenschutzrecht im Bereich der Medizin aufgehoben oder zumindest stark qualifiziert werden. Diskriminierung, Stigmatisierung und der Missbrauch von Gesundheitsdaten werden durch unerwünschte Verwendungen von Daten hervorgerufen ▸

DATENSCHUTZPRAXIS/MEDIZIN

und nicht durch Datenerhebung oder die meisten anderen Formen von Datenverarbeitung an sich. Datenerhebung ist nicht der eigentliche Verursacher, z. B. von Diskriminierung, und kann im Gegenteil bei der Bekämpfung von Diskriminierung helfen (indem Diskriminierung systematisch erfasst und analysiert wird).

2. Kein Eigentum an Patientendaten

Ein falscher Weg wäre es, Patienten Eigentumsrechte an den sie betreffenden (Gesundheits-) Daten einzuräumen. Nach diesem gesetzgeberisch nunmehr scheinbar angestrebten Konzept eines ‚Dateneigentums' sollen Patienten über eigene Daten verfügen, indem sie Verträge schließen oder Rechte abtreten. Gegen diese Idee sprechen gewichtige verfassungsrechtliche und rechtspolitische Gründe.

3. Datensicherheit verbessern

Mittelbaren Auswirkungen der Datenverarbeitung lässt sich vor allem durch eine Verbesserung der Datensicherheit begegnen. Gesundheitsdaten müssen so gespeichert und übermittelt werden, dass ein unbefugter Zugriff durch Dritte ebenso verhindert wird wie ein Verlust der Daten. Hierbei ist wiederum zu berücksichtigen, dass effektive Datensicherheit in der Regel zusätzliche Datenverarbeitung erfordert, um Sicherheitsverstöße und Verursacher zu erkennen, zu melden und zu bekämpfen, um Nachforschungen in Datenpannen zu ermöglichen und um künstliche Intelligenz zu trainieren. Dies ist ein weiterer Grund, Datenerhebungsverbote im europäischen Datenschutzrecht zu lockern und Sparsamkeits- und Löschungsgebote zu relativieren oder abzuschaffen zugunsten verbesserter Datensicherheit.

4. Allgemeine elektronische Gesundheitsakte und Einwilligungen einführen

Um Gesundheitsdaten effektiv zu nutzen, bietet sich die Einrichtung einer persönlichen allgemeinen Patientenakte an, die unabhängig von einer bestimmten Institution geführt wird. Vorbild könnten hier die skandinavischen Länder sein, die derartige Systeme bereits etabliert haben.

5. Anforderungen an freiwillige Einwilligung flexibler handhaben

Damit Patienten nicht das Gefühl bekommen, ein unpersönlicher Anwendungsfall oder Objekt der Medizin zu sein, sollte eine freiwillige Entscheidung des Betroffenen bzgl. der Datenverarbeitung so oft wie möglich vorgesehen werden. Allerdings muss eine solche Entscheidung nicht wie bisher in Form einer differenziert erklärten Einwilligung aufgrund einer ausführlichen Belehrung dokumentiert werden, sondern könnte auch in standardisierter Kurzform erfolgen, wie z. B. bei der Zugriffsvermittlung auf eine allgemeine Gesundheits- oder Patientenakte. Ebenso könnten für komplexe Sachveralte Sonderregelungen geschaffen werden, wie z. B. die in der DSGVO für Forschungszwecke angelegte Einführung einer Schrankenregelung, welche die Datenverarbeitung zu bestimmten medizinischen Zwecken freistellt. Nach geltendem Recht wäre eine derartige Regelung allerdings nur auf Ebene der EU-Mitgliedsstaaten möglich, was eine Rechtszersplitterung befürchten lässt, die eine international betriebene Forschung behindern würde.

Was medizinische Forschung betrifft, sollten unter bestimmten Umständen vergleichsweise weit formulierte Einwilligungserklärungen regelmäßig anerkannt werden, die derzeit bei datenschutzrechtlicher Betrachtung mit Unsicherheit behaftet sind. Die gleiche Problematik gilt für die medizinische Versorgung in Fällen der Einbeziehung von Algorithmen oder datenaggregierender Apps, die einen Datenabgleich zur Abklärung oder Vorbeugung eines gerade unbekannten medizinischen Zustandes vornehmen.

Vor diesem Hintergrund werden unter Begriffen des »broad consent«, »open consent« oder eines »dynamic consent« (Steinsbekk et al. 2013) neue Einwilligungsmodelle diskutiert. Es wird teilweise vorgeschlagen, jede neue Nutzung und jeden neuen Zugriff auf Gesundheitsdaten durch den Patienten einzeln autorisieren zu lassen, um so dem Gefühl eines Kontrollverlusts durch den Patienten entgegenzuwirken. Um eine ‚Erschöpfung' des Patienten durch Überinformation oder eine Unmöglichkeit der Autorisierung durch verstorbene Patienten zu verhindern, müsste aber der Entscheidungsprozess standardisiert und vereinfacht werden und hierzu z. B. eine allgemeine Einwilligung zu Beginn der Datenverwendung ohne explizite Rückkopplung und Re-Autorisierung im Interesse von Medizinern und Patienten vorgesehen werden.

Eine erleichtere Nutzung von Gesundheitsdaten zu Forschungszwecken erfordert auch eine flexiblere Handhabung der Einwilligung der Studienteilnehmer. Weder der medizinischen Praxis noch den einzelnen Patienten ist mit langen, hochkomplexen Einwilligungsformularen gedient, die schwerlich jeden vorstellbaren Einzelfall abdecken können. Der geltenden Rechtslage ist die Einräumung einer ‚weiten Einwilligung' noch fremd, sodass gerade im europäischen Datenschutzrecht Gesetzesänderungen nötig sind. Eine »bereichsspezifische Einwilligung«, d.h. vom Normallfall der fallspezifischen Einwilligung abweichend und auf bestimmte Bereiche der Medizin (Überwachung von Gesundheitsdaten allgemein, Behandlung von X, Forschung von Y), würde die Datenverarbeitung zu medizinischen Zwecken erleichtern. Ihre Einführung sollte für bestimmte, besonders vertrauenswürdige Einrichtungen, besonders nützliche Verwendungszwecke oder relativ ungefährliche Datensätze erwogen werden.

6. Vertrauenswürdigkeit durch Zertifizierung steigern

Während Patienten einer Datenverarbeitung wie dem Anlegen einer Patientenakte im Rahmen eines Arztbesuchs Vertrauen entgegenbringen, fällt dies bei ‚im Verborgenen', d.h. ohne direkte Interaktion mit dem Patienten, betriebener Datenverarbeitung schwerer. Ist der Umgang mit den eigenen Daten für den Patienten nicht im Einzelnen erkennbar, muss der Patient Vertrauen in die datenverarbeitende Einrichtung aufbringen. Eine Vertrauensbasis für die medizinische Datenverarbeitung kann sich aus den Regularien des Projekts und insbesondere der Umgebung der Datenverarbeitung ergeben. Die Beurteilung dieser Faktoren durch den Betroffenen verlangt dabei ein ausreichendes Maß an Transparenz in die Strukturen.

Möglich wäre es daher, die Verarbeitung von Gesundheitsdaten in Netzwerke aus staatlich (z.B. durch Datenschutzbehörden) zertifizierten vertrauenswürdigen Akteuren des Gesundheitssystems wie Ärzten, Krankenhäusern, Krankenkassen und Forschungsinstitutionen zu verlagern. Im Gegenzug für eine Zertifizierung könnten die beteiligten Institutionen von einem Absenken einzelner datenschutzrechtlicher Anforderungen an die Einwilligungserklärung profitieren. Vor Bereitstellung seiner Gesundheitsdaten wäre von dem Patienten eine bereichsspezifische, d.h. auf bestimmte Forschungsprojekte oder Bereiche der Medizin beschränkte Einwilligung in eine Datenverarbeitung abzugeben. Der Gedanke einer derartigen Einwilligung ist in Erwägungsgrund 33 der DSGVO auch in rechtlicher Hinsicht bereits angelegt.

Die Zertifizierung stünde Einrichtungen offen, die eine besondere Integrität nachweisen können und wäre mit regelmäßigen Rechenschaftspflichten und Überprüfungen hinsichtlich der Dokumentation von Zielen und Rahmenbedingungen der Datenverarbeitung im Hinblick auf Zugang, Verwendung und Kontrollmechanismen verbunden. Eine Datenverarbeitung in Widerspruch zu den Bedingungen des Netzwerks unterläge einem Entzug der Lizenz sowie zivil- und strafrechtlicher Verfolgung, um eine Einhaltung der Regeln über die Datenverarbeitung zu sichern und das Vertrauen der Patienten zu stärken (Mittelstadt u. Floridi 2016).

7. Einschränkung von Betroffenenrechten bei namenlosen Daten

Die nach geltendem Datenschutzrecht Betroffenen zustehenden Rechte auf Zugang und Löschung können für die medizinische Forschung erheblichem Aufwand verursachen und die Integrität der gespeicherten Daten gefährden. Aus diesem Grund sollten Betroffenenrechte für den Fall einer Forschung mit Gesundheitsdaten, die den Namen des Betroffenen nicht beinhalten, eingeschränkt werden. Ähnlich der Problematik bei der Einwilligung in eine Datenverarbeitung zu medizinischen Zwecken dürfte es in vielen Fällen bereits an den Fachkenntnissen und Einblicken des Patienten in die Datenverarbeitung fehlen und so eine sinnvolle Rechtsausübung ausscheiden.

Über den Autor

Prof. Dr. Lothar Determann
Praktiziert und lehrt internationales Technologie- und Wirtschaftsrecht in Kalifornien und Deutschland
Als Partner bei Baker & McKenzie LLP in Palo Alto berät Lothar Determann Unternehmen bezüglich globaler Geschäftsexpansion, geistiges Eigentum, Datenschutz und Verträge. Er ist als Rechtsanwalt in Deutschland und Kalifornien zugelassen.

Lothar Determann ist Mitglied der Vereinigung Deutscher Staatsrechtslehrer und außerplanmäßiger Professor an der Freien Universität Berlin, wo er sich 1999 habilitiert hat, und hält regelmäßig Vorlesungen zum Thema Datenschutz, Computer- und Internetrecht ab, an der University of California, Berkeley School of Law (jährlich seit 2004), am Hastings College of the Law (seit 2010) und an der Stanford Law School (2011).

Er hat mehr als 120 Aufsätze in juristischen Fachzeitschriften und 6 Bücher veröffentlicht. California Privacy Law – Practical Guide and Commentary, 3. Auflage 2018 behandelt U.S.-Bundesrecht und kalifornisches Datenschutzrecht ausführlich. Determann's Field Guide to Privacy Law (3. Auflage 2017) ist auch in chinesischer, japanischer, russischer und deutscher Sprache erschienenen: Datenschutz - International Compliance Field Guide, C.H. Beck, München, 2017

AUFSICHTSBEHÖRDEN

ERSTE PRÜFUNGEN IM RAHMEN DER DSGVO – DIE QUERSCHNITTSPRÜFUNG DER LFD NIEDERSACHSEN

Barbara Thiel

Der 25. Mai 2018 war ein Tag, mit dem Datenschützer in der gesamten Europäischen Union hohe Erwartungen verknüpften. Nach einem jahrelangen Gesetzgebungsprozess mit vielen Diskussionen und Kompromissen sowie einer zweijährigen Übergangszeit erreichte die europäische Reform des Datenschutzrechts ihren vorläufigen Höhepunkt: Die Datenschutz-Grundverordnung (DSGVO) galt jetzt in allen Mitgliedstaaten der EU und sorgte damit dafür, dass der rechtliche Flickenteppich in Sachen Datenschutz von nun an Geschichte war.

Doch das historische Werk der DSGVO verursachte auch neue Aufwände, wie es bei umfassenden Gesetzesreformen immer der Fall ist. Das galt nicht nur für die verantwortlichen Verarbeiter von Daten, welche vor allem den Umfang von Informations- und Dokumentationspflichten mal lauter mal leiser beklagten, sondern auch für die Datenschutzaufsichtsbehörden, die für die Durchsetzung der Verordnung zuständig sind. Insofern war es auch für die Landesbeauftragte für den Datenschutz Niedersachsen (LfD) keine Überraschung, dass sich die Anfragen zum neuen Gesetz rund um dessen Geltungsbeginn erhöhten. Wie enorm dieser Anstieg letztlich ausfiel, war allerdings nicht vorhersehbar. In manchen Bereichen stiegen die Eingänge um mehrere 100 Prozent, besonders kleine und mittelständische Unternehmen, Arztpraxen und gemeinnützige Vereine wollten wissen, was sie nun zu tun hatten. In dieser Zeit galt es hauptsächlich, in kurzer Zeit möglichst viele Anfragen zu bearbeiten. Eine schnelle Reaktion war das Gebot der Stunde.

Proaktives Handeln statt Passivität

Allerdings – und diesem Aspekt sollte ebenfalls Rechnung getragen werden – gehört es zu den Kernkompetenzen einer Datenschutzaufsichtsbehörde, die korrekte Anwendung der DSGVO zu überwachen und durchzusetzen. Nicht umsonst wird dieser Punkt in Art. 57 Abs. 1 DSGVO als erste Aufgabe der Aufsicht genannt. Deshalb veranlasste die LfD Niedersachsen Ende Juni 2018 eine anlasslose Prüfung von 50 großen und mittelgroßen niedersächsischen Unternehmen zur Umsetzung der DSGVO, die bisher größte Prüfung in der Geschichte der Behörde.

Im Vordergrund dieser sogenannten Querschnittsprüfung stand allerdings nicht der reine Kontrollaspekt, sondern eine Ist-Analyse über den Umsetzungsstand der neuen Regeln in Niedersachsen. Falsche Anwendungsfälle und Defizite sollten zwar gegenüber den geprüften Unternehmen benannt werden, waren aber nicht das Hauptmotiv für die Durchführung der Prüfung. Stattdessen war es das vorrangige Ziel, eine ehrliche Bestandsaufnahme darüber zu erhalten, wie gut die DSGVO bereits in der Praxis verankert war. Diese sollte vor allem zeigen, in welchen Bereichen es noch Handlungs-, Aufklärungs- und Nachbesserungsbedarf gab.

Im Sinne von Aufklärung und Sensibilisierung – eine der neuen in der DSGVO verankerten Aufgaben der Aufsichtsbehörden – sollte darüber hinaus ganz allgemein das Bewusstsein der Verantwortlichen für die Bedeutung des Datenschutzes gestärkt werden. Trotz dieser Zielsetzung war aber auch von vorneherein klar, dass gravierende Verstöße geahndet würden, falls diese im Rahmen der Prüfung zutage treten sollten.

Sorgfältige Auswahl der zu prüfenden Unternehmen

Großer Wert wurde auf eine sinnvolle Auswahl der zu prüfenden Unternehmen gelegt. Die Wahl fiel schließlich auf 20 große und 30 mittelgroße Firmen, bei denen aufgrund ihrer Größe davon ausgegangen werden konnte, dass bereits eine funktionierende Datenschutzorganisation vorhanden sein müsste und die Umsetzung der DSGVO dort dementsprechend frühzeitig in Angriff genommen worden war. Kleine und mittlere Betriebe sollten dagegen gerade nicht Teil der Querschnittsprüfung sein, da es dort sowieso erkennbar noch viel Beratungsbedarf gab.

In die konkrete Auswahl der Unternehmen flossen die folgenden Aspekte mit ein:

- Erstens sollte die Prüfung das gesamte Flächenland Niedersachsen abbilden, mit Unternehmenssitzen von der Küste bis nach Göttingen, von Osnabrück bis Helmstedt.
- Zweitens sollten die ausgewählten Unternehmen nicht nur Daten ihrer Beschäftigten verarbeiten, sondern auch Kundendaten – möglichst aus dem Consumer-Bereich.
- Drittens wurde die Prüfung branchenübergreifend angelegt. Unter den ausgewählten Unternehmen waren dementsprechend Firmen aus der Versicherungswirtschaft, dem Finanzbereich und dem Handel genauso vertreten wie Versorgungsunternehmen oder Wach- und Schließgesellschaften.
- Viertens sollten »Doppelbelastungen« vermieden werden. Unternehmen, die bereits vor Kurzem in einem anderen Rahmen geprüft worden waren, blieben deshalb dieses Mal unberücksichtigt.
- Fünftens sollten die Firmen eine Größe haben, die zur Bestellung eines Datenschutzbeauftragten verpflichtet.

Offene Fragen zu zehn Themenkomplexen

Die 50 ausgewählten Unternehmen erhielten einen Fragebogen mit insgesamt zehn Themenkomplexen, welche die für Verantwortliche wesentlichen Bereiche der DSGVO ansprechen. Konkret handelte es sich um das Verzeichnis von Verarbeitungstätigkeiten, die Rechtsgrundlagen für die Datenverarbeitung, die Betroffenenrechte, den technischen Datenschutz, die Datenschutz-Folgenabschätzung, die Auftragsverarbeitung, die Bestellpflicht für Datenschutzbeauftragte, die Pflicht zur Meldung von Datenschutzverletzungen nach Art. 33 DSGVO und die Rechenschaftspflicht. Der Fragebogen beruhte auf einer Checkliste zur DSGVO für kleinere Unternehmen, welche die LfD Niedersachsen bereits im November 2017 veröffentlicht hatte. Diese Liste sollte Unternehmen dabei helfen, selbst einschätzen zu können, wie weit die Umsetzung der Verordnung bei ihnen zum damaligen Zeitpunkt vorangeschritten war.

Ganz bewusst wurden die Fragen an die Unternehmen möglichst offen gehalten. Das eröffnete zum einen den Befragten die Möglichkeit, Antworten zu verfassen, die ihrer konkreten Größe und Situation angemessen sind. Zum anderen lassen Antworten auf offene Fragen sehr viel bessere Rückschlüsse darauf zu, inwieweit die Anforderungen der DSGVO tatsächlich bereits in die alltäglichen Unternehmensprozesse integriert sind und nicht nur sporadisch, sondern kontinuierlich umgesetzt werden.

Ebenso bewusst wurde darauf verzichtet, die Erfüllung rechtlicher Vorgaben kleinteilig abzufragen, da der Antwortende dadurch zwangsläufig in eine bestimmte Richtung geführt wird. Bei dieser Art der Fragestellung ist anhand der Antworten nicht mehr unbedingt erkennbar, ob der Befragte auch selbstständig an alle Details gedacht hätte. Mit dem gewählten Ansatz müssen die Befragten dagegen den Lösungsweg eigenverantwortlich darstellen und zeigen damit zugleich, dass sie sich mit den angesprochenen Themen ernsthaft auseinander gesetzt haben.

Natürlich war diese Methode für die geprüften Unternehmen aufwändiger als einen Multiple-Choice Fragebogen auszufüllen. Doch dafür waren die Antworten auch weit ▸

aussagekräftiger als es ein paar Kreuze und Häkchen hätten sein können. Sie machen deutlich, wo das Thema DSGVO wirklich angekommen ist und wo es noch eher eine Randerscheinung ist.

Auswertung anhand von 200 Kriterien

Als besondere Herausforderung stellte sich die Auswertung der eingesandten Antworten dar. Teilweise reichten die Unternehmen mehrere hundert Seiten Unterlagen ein. Ein Katalog mit circa 200 Auswertungskriterien sollte dabei helfen, den Überblick zu behalten und die Antworten einheitlich zu bewerten. Die gewählten Kriterien machen sehr detailliert deutlich, was ein Verantwortlicher alles zu beachten hat, um datenschutzkonform aufgestellt zu sein. Daher wird der Katalog nach Abschluss der Querschnittsprüfung veröffentlicht und so allen Interessierten zugänglich gemacht.

Als Bewertung der jeweiligen Kriterien waren drei Ausprägungen möglich:

1. Das Kriterium ist erfüllt
2. Das Kriterium ist nicht erfüllt
3. Das Kriterium ist teilweise erfüllt

Anschließend wurden alle Einzelkriterien eines Fragenkomplexes zu einer Gesamtbewertung zusammengefasst und dem Komplex eine entsprechende Ampelfarbe zugeordnet: Rot, Gelb oder Grün. »Grün« erhielten die Komplexe, die weitestgehend angemessen beantwortet wurden und bei denen kein konkreter Handlungsbedarf gesehen wurde. Als »Gelb« wurden die Bereiche eingestuft, bei denen es noch Handlungsbedarf gibt. Das ist dann der Fall, wenn die Einzelkriterien häufiger mit »teilweise« oder bisweilen auch mit »nein« bewertet werden mussten. »Rot« erhielten schließlich die Komplexe, bei denen die Antworten auf erheblichen Handlungsbedarf schließen ließen, also die Einzelkriterien überwiegend mit »teilweise« und »nein« bewertet wurden.

Transparenz gegenüber den Geprüften

Alle geprüften Unternehmen haben inzwischen ihre schriftlichen Prüfergebnisse erhalten. Für die, denen insgesamt die Farben Grün oder Gelb zugeordnet worden sind, ist die Querschnittsprüfung damit beendet. Jedes Unternehmen hat auch den detaillierten Kriterienkatalog mit der Bewertung jedes einzelnen Kriteriums erhalten. So können die Unternehmen transparent nachvollziehen, welcher Maßstab an die Antworten angelegt wurde und wie es zur Gesamtbewertung der zehn Fragenkomplexe gekommen ist. Zugleich haben sie auf diese Weise konkrete Hinweise auf Verbesserungspotenziale bekommen.

Auch die insgesamt mit »Rot« bewerteten Unternehmen haben ihre Ergebnisse schriftlich erhalten. Für sie war dies allerdings aufgrund der erheblichen Handlungsbedarfe nur ein Zwischenschritt. Zugleich wurden sie dazu aufgefordert, zu den Ergebnissen und den erkannten Defiziten Stellung zu nehmen. Diese Stellungnahmen sind zwischenzeitlich eingetroffen, waren aber zum Redaktionsschluss dieses Artikels noch nicht vollständig ausgewertet. Sollte es auch mithilfe dieser erneuten Stellungnahmen nicht möglich sein, die Sachlage in den jeweiligen Unternehmen zufriedenstellend zu beurteilen, werden weitergehende Kontrollmaßnahmen im Rahmen von Vor-Ort-Terminen stattfinden müssen. Diese werden hauptsächlich dazu dienen, die gewonnenen Erkenntnisse in einem persönlichen Gespräch zu erläutern und gemeinsam mit den Unternehmen zu erörtern, wo noch erheblicher Handlungsbedarf gesehen wird. Es bleibt abzuwarten, wie die Unternehmen darauf reagieren und inwieweit sie bereit sind, etwaige Verstöße abzustellen. Es ist nicht auszuschließen, dass es in Einzelfällen auch zur Verhängung eines Bußgelds kommen kann, je nachdem, wie schwerwiegend der jeweilige Verstoß ist und wie das Unternehmen damit umgegangen ist.

Erster Einblick in die Ergebnisse

Der für die Öffentlichkeit bestimmte Abschlussbericht lag zum Redaktionsschluss dieses Beitrags noch nicht vor, dennoch können bereits jetzt einige ausgewählte Ergebnisse genannt werden. Zunächst das Positive: Es gab einige Bereiche, zu denen weitgehend zufriedenstellende Antworten eingereicht wurden. Das betraf etwa die Fragenkomplexe zur Auftragsverarbeitung, zu Datenschutzbeauftragten, zur Meldepflicht von Datenschutzverletzungen oder zu den Dokumentationspflichten. Letzteres ist ein gutes Zeichen dafür, dass die Verantwortung für die Umsetzung der Datenschutzregeln tatsächlich erkannt und ernst genommen wird. Schließlich trifft die Verantwortlichen durch die DSGVO eine erweiterte Rechenschaftspflicht. Sie müssen im Streitfall glaubhaft nachweisen können, dass sie die Pflichten und Anforderungen der Verordnung erfüllen. Zwar war der Grundsatz der Rechenschaftspflicht bereits in der früheren Datenschutzrichtlinie enthalten, neu hinzugekommen in der DSGVO ist aber die damit verbundene Nachweispflicht, womit dem Datenverarbeiter allgemein mehr Eigenverantwortung auferlegt worden ist.

Erhebliche Defizite bei technisch-organisatorischen Maßnahmen

Wenig überraschend gab es aber natürlich auch Komplexe mit deutlichen Defiziten. Das betraf unter anderem das Verzeichnis der Verarbeitungstätigkeiten (VVT). So blieben hier Aktualisierungsprozesse teilweise unklar, Standardverfahren waren bisweilen nicht erkennbar oder es fehlten wichtige Kontaktangaben. Mit diesen Mängeln wird der Bedeutung des VVT nicht hinreichend Rechnung getragen. Denn ist dieses mit Fehlern behaftet, fehlt im Unternehmen eindeutig die erforderliche Prozesskontrolle.

Ein weiteres Problemfeld waren die Betroffenenrechte, was besonders an der unzureichenden Erfüllung der Informationspflichten nach Art. 13 und 14 DSGVO lag. So hatten die Unternehmen zum Teil lediglich Mustertexte zur Information kopiert, ohne diese an das jeweilige Unternehmen und seine Verarbeitungsprozesse anzupassen. Häufig wurden zudem nur beispielhaft Verarbeitungszwecke genannt, sodass die betroffene Person am Ende nicht über die konkreten Vorgänge informiert wurde. Ebenso war die Information zu einer Übermittlung in Drittstaaten außerhalb der EU häufig unsauber formuliert oder nur aus dem Gesetz abgeschrieben. Die betroffenen Unternehmen müssen hier dringend nachbessern. Denn wenn die Betroffenenrechte nicht angemessen erfüllt werden, setzt sich die Machtasymmetrie zwischen Verantwortlichen und Betroffenen, welche die DSGVO auszugleichen versucht, dauerhaft fest.

Ein dritter Bereich, in dem erhebliche Defizite festgestellt wurden, ist jener der technisch-organisatorischen Maßnahmen (TOM). Gefragt war hier unter anderem, wie die Unternehmen sicherstellen, dass ihre TOM bzw. die ihrer Dienstleister ein dem Verarbeitungsrisiko angemessenes Schutzniveau gewährleisten. Oder wie sie dafür sorgen, dass diese Maßnahmen an den jeweiligen Stand der Technik angepasst werden. Die Antworten waren hier bedauerlicherweise dürftig, was umso kritikwürdiger ist, als dass ohne angemessene TOM die Sicherheit der Verarbeitung im Sinne von Art. 32 DSGVO nicht gewährleistet ist.

Konsequenzen für die Arbeit der LfD Niedersachsen

Die Querschnittsprüfung hat äußerst interessante Einblicke zur Umsetzung der DSGVO in niedersächsischen Unternehmen geliefert. Aber natürlich kann dies nur der Anfang sein; weitere anlasslose Kontrollen werden folgen, um der Aufgabe der LfD Niedersachsen als Aufsichtsbehörde angemessen nachzukommen. Ausgehend von den beschriebenen Ergebnissen werden sich diese weiterführenden Prüfverfahren und Schwerpunktprüfungen vor allem auf die besonders auffälligen Bereiche wie den der TOM konzentrieren.

Andererseits sollen die gewonnenen Erkenntnisse auch dazu genutzt werden, die notwendige Sensibilisierung und Aufklärung weiter voranzutreiben. So werden vorrangig zu den Komplexen neue Handreichungen und Hilfestellungen entstehen, in denen offensichtlich noch großer Nachholbedarf besteht. Zudem können Unternehmen, die hinsichtlich der DSGVO-Umsetzung noch immer unsicher sind, den Fragen- und Kriterienkatalog als Richtschnur für ihr zukünftiges Handeln verwenden.

Über die Autorin

Babara Thiel

Landesbeauftragte für den Datenschutz des Landes Niedersachsen

AUFSICHTSBEHÖRDEN

EIN SCHRITT ZUR VERBESSERTEN TRANSPARENZ FÜR ALLE – DER „DATENSCHUTZ-STECKBRIEF“

Marit Hansen und Angelika Martin,
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein[1]

1. Transparenz in der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung nennt nicht nur als einen der fundamentalen Datenschutz-Grundsätze „Transparenz“ (Artikel 5 Absatz 1 Buchstabe a DSGVO), sondern enthält auch in vielen Artikeln die Forderung, dass die Verantwortlichen in geeigneter Form über die Datenverarbeitung informieren müssen. Es ist notwendig, dass die betroffenen Personen verstehen können, wie ihre personenbezogenen Daten verarbeitet werden. Ähnliches gilt im Falle der Benachrichtigung nach einer Verletzung des Schutzes personenbezogener Daten (Artikel 34 DSGVO), in dem ein Verständnis dazu nötig ist, welche Risiken für Rechte und Freiheit bestehen und welche Maßnahmen die nachteiligen Auswirkungen abmildern können.

So steht in Artikel 12 DSGVO:

> *„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.“ (Artikel 12 Absatz 1 Satz 1 DSGVO).*
>
> *Für die Zukunft haben sich die Macher der DSGVO standardisierte Bildsymbole vorgestellt, wie dies Artikel 12 Absatz 7 Satz 1 DSGVO beschreibt: „Die Informationen, die den betroffenen Personen gemäß den Artikeln 13 und 14 bereitzustellen sind, können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.“*

Zu den Nutzen und den Herausforderungen in Bezug auf Bildsymbole (Icons, Piktogramme) gibt es schon seit Jahrzehnten Ausarbeitungen, auch mit Beteiligung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)[2]. Es ist gar nicht so einfach, geeignete Bildsymbole zu entwickeln, die aus sich heraus verständlich sind und vor allem nicht fehlinterpretiert werden, selbst wenn sie mit dem Informationstext kombiniert werden. Der nötigen Entwicklung, der Diskussion und schließlich der Standardisierung wollen wir nicht vorgreifen – dennoch können Verantwortliche auch jetzt schon bei ihrer Informationspflicht die Textverständlichkeit durch visuelle Elemente unterstützen. Dies ist die Grundlage für den Vorschlag des „Datenschutz-Steckbriefs“ aus dem ULD.

2. Herausforderungen beim Umsetzen der Informationspflichten

Es ist nicht einfach, betroffene Personen über die Verarbeitung ihrer personenbezogenen Daten in den verschiedenen Verarbeitungstätigkeiten so zu informieren, dass sie

- in einer präzisen und verständlichen Form vorliegen,
- in einer einfachen Sprache geschrieben sind und
- möglichst mit visuellen Elementen so aufbereitet werden, dass die Informationen leicht wahrzunehmen sind und sie anhand der Grafiken gut den Informations- und Mitteilungspflichten der Artikel 13 bis 22 DSGVO zugeordnet werden können.

Weiterhin ist die Gruppe der betroffenen Personen nicht homogen. Sie setzt sich aus Menschen unterschiedlichster Persönlichkeiten und Lebensumstände zusammen. Dabei kann es sich beispielsweise um Personen handeln,

- die Datenschutz für sich zwar wichtig empfinden, aber nicht die Zeit haben bzw. sich nicht die Zeit nehmen die Datenschutzerklärungen sorgfältig zu lesen,
- die in Bezug auf das Thema Datenschutz hochinteressiert und gebildet sind und ihre Rechte ganz genau und detailliert nachlesen,
- die den Datenschutz als unwichtig empfinden und der Meinung sind nichts zu verbergen zu haben,
- für die Deutsch nicht die Muttersprache ist sowie
- Menschen, für die formale Texte schwierig zu verstehen sind (etwa für Kinder).

Alle diese Menschen können betroffene Personen sein und sollen anhand der Informationen, die die verantwortliche Stelle für sie herausgibt, verstehen können, welche Daten von ihnen wie verarbeitet werden.

Aus den Rückmeldungen von betroffenen Personen sind die üblichen langen und kompliziert zu lesenden Datenschutzerklärungen der Verantwortlichen seit der Einführung der DSGVO im Mai 2018 nicht der richtige Weg, um der Informationspflicht nachzukommen und alle betroffenen Personen angemessen zu informieren. Menschen neigen dazu – wenn sie diese Art von Datenschutzerklärungen überhaupt lesen – diese zu überfliegen und aufgrund ihrer Länge und Komplexität einfach „wegzuklicken“ – und das ist nicht das, was mit der Information erreicht werden soll.

3. Vorschlag: „Datenschutz-Steckbrief“

Um die Informationspflichten in Zusammenhang mit Verarbeitungstätigkeiten zu erfüllen, verwendet das ULD zusätzlich einen „Datenschutz-Steckbrief“, wie er in Abbildung 1 dargestellt wird.

Der „Datenschutz-Steckbrief“ soll in Verbindung mit einem dreistufigen Konzept im besten Fall alle betroffenen Personen verständlich informieren: kurz und prägnant, in einer einfachen Form und Sprache sowie durch grafische Elemente unterstützt. Eine mehrstufige Information, d. h. je nach gewünschtem Detaillierungsgrad, hat die Artikel-29-Datenschutzgruppe bereits im Jahr 2004 empfohlen[3] und dies vor kurzem auch für den DSGVO-Kontext bestätigt[4].

Der „Datenschutz-Steckbrief“ ist auf der obersten Ebene innerhalb einer Methodik angesiedelt, mit der die Informationspflicht in öffentlichen und nichtöffentlichen Stellen umgesetzt und die gesamte Gruppe der betroffenen Personen angesprochen werden kann.

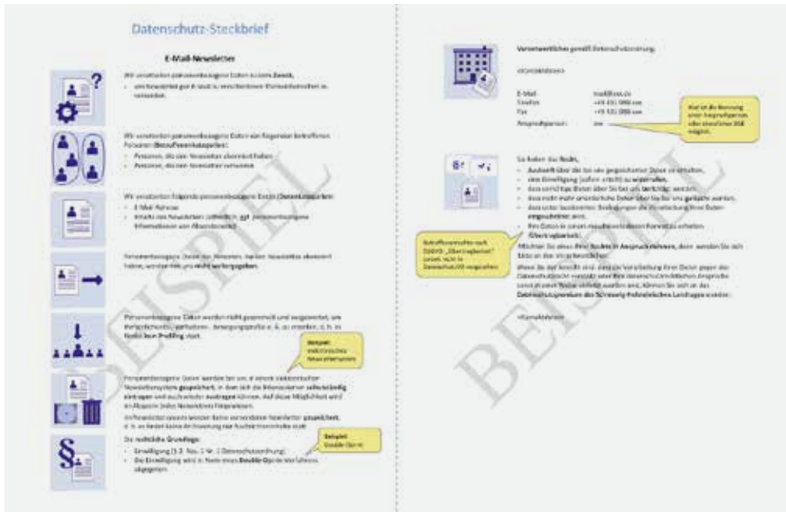


Abb. 1: Vorschlag für einen „Datenschutz-Steckbrief“

Abbildung 2 visualisiert die Umsetzung der Informationspflicht:

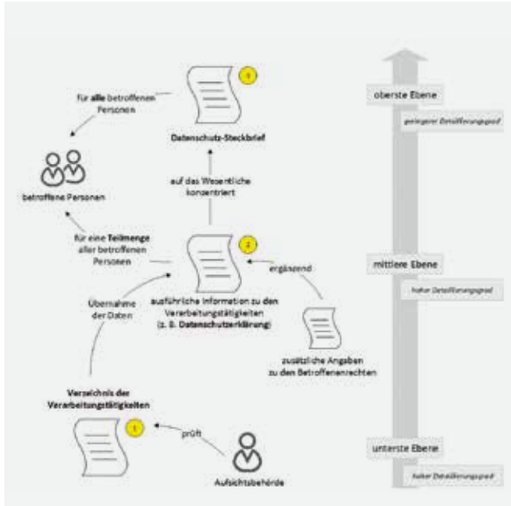


Abb. 2: Dreistufenkonzept „Datenschutz-Steckbrief“

Auf der untersten Ebene (Punkt 1 in der Abbildung) werden zunächst die Verarbeitungstätigkeiten in einer Organisation erfasst und zum Verzeichnis der Verarbeitungstätigkeiten zusammengeführt. Dieses Dokument stellt die Basis für die Umsetzung der Informationspflichten dar, da in diesem die meisten Informationen davon enthalten sind, die den betroffenen Personen zur Verfügung gestellt werden müssen. Weiterhin ist dieses Verzeichnis sowohl ein Pflichtnachweis nach Artikel 30 DSGVO als auch ein Baustein bei der Verarbeitungsdokumentation.[5] Auf dieser Ebene wird mit einem hohen Detaillierungsgrad gearbeitet. ▸

[1] Dieser Text basiert auf der Kurzdarstellung in Textziffer 6.1.4 „Der Datenschutz-Steckbrief zur Umsetzung der Informationspflicht“ im 37. Tätigkeitsbericht des ULD.

[2] Hansen: Putting Privacy Pictograms into Practice – A European Perspective, in: Informatik 2009 – Im Focus das Leben, LNI P-154, Bonn 2009, S. 1703-1716;
Holtz, Nocun, Hansen: Towards displaying privacy information with icons, in: Proc. Summer School on Privacy and Identity Management, AICT 352, 2011, S. 338-348.

[3] Artikel-29-Datenschutzgruppe: „Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten“, WP 100, angenommen am 25. November 2004, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp100_de.pdf

[4] Artikel-29-Datenschutzgruppe: „Leitlinien für Transparenz gemäß der Verordnung 2016/679“, WP 260 rev.01, angenommen am 29. November 2017, zuletzt überarbeitet und angenommen am 11. April 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

[5] Um das Verzeichnis der Verarbeitungstätigkeiten zu erstellen, kann die ULD-Vorlage verwendet werden: https://www.datenschutzzentrum.de/dokumentation/

Auf der mittleren Ebene (Punkt 2 in der Abbildung) werden den betroffenen Personen ausführliche Informationen in einem hohen Detaillierungsgrad zur Verfügung gestellt. Die Basis dieser Information sind die Angaben aus dem Verzeichnis der Verarbeitungstätigkeiten, die um zusätzliche Angaben entsprechend den Artikeln 13 bis 22 DSGVO ergänzt werden. Diese ausführlichen Informationen können den betroffenen Personen beispielsweise in Form einer Datenschutzerklärung auf der Organisationswebseite zur Verfügung gestellt werden, oder das Verzeichnis der Verarbeitungstätigkeiten wird so geschrieben, dass es – ergänzt um die oben genannten zusätzlichen Angaben – veröffentlicht werden kann. Diese Ebene spricht die betroffenen Personen an, die sich umfassend und ausführlich über ihre Rechte informieren möchten.

Auf der obersten Ebene (Punkt 3 in der Abbildung) wird allen betroffenen Personen mit dem „Datenschutz-Steckbrief" eine leicht verständliche und kompakte Übersicht aller Informationen gegeben, die ihnen gemäß der DSGVO zur Verfügung gestellt werden müssen. Die Informationen können der mittleren Ebene entnommen werden. Die Herausforderung liegt in der (Um-)Formulierung der Inhalte. So sollten die Informationen kurz und prägnant beschrieben werden, sich auf das Wesentliche konzentrieren und in einer klaren und einfachen Sprache verfasst werden.

6 Siehe Fußnote 4.

7 https://klartext.uni-hohenheim.de/hix

8 https://klartext.uni-hohenheim.de/klartext-checkliste

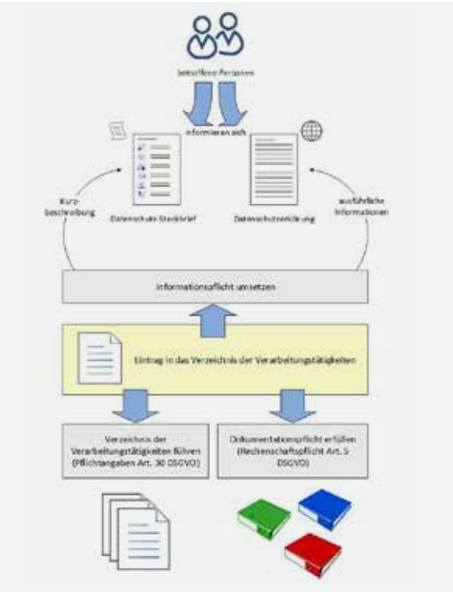


Abb. 3: Elemente zur Umsetzung der Informations- und Rechenschaftspflicht

Die Vorlage des „Datenschutz-Steckbriefs" gibt weiterhin grafische Elemente vor, die frei verwendet werden können. Diese Ebene spricht mit dem „Datenschutz-Steckbrief" alle betroffenen Personen an, die sich mithilfe der einheitlichen und wiedererkennbaren Bildsymbole sowie der einfachen und verständlichen Sprache schnell und strukturiert über die Verwendung ihrer Daten informieren möchten.

Die Vorlage des „Datenschutz-Steckbriefs" kann auf der ULD-Webseite heruntergeladen werden: www.datenschutzzentrum.de/dokumentation/

4. Dokumentation – sowohl zur Informations- als auch zur Rechenschaftspflicht

Die nachfolgende Abbildung zeigt die Bedeutung eines einzelnen Eintrags für das Verzeichnis der Verarbeitungstätigkeiten als zentrales Dokument und als Informationsbasis zur Umsetzung der Informationspflicht. Sie gibt aber auch einen Überblick über die zwei weiteren Einsatzbereiche des Einzeleintrags sowohl als Dokumentationsbestandteil zur Umsetzung der Rechenschaftspflicht als auch als Bestandteil im Verzeichnis der Verarbeitungstätigkeiten.

5. Ergebnis

Der „Datenschutz-Steckbrief" unterstützt den Verantwortlichen in der Pflicht zur einfachen und verständlichen Information. Durch eine mehrstufige Informationsstrategie können die betroffenen Personen zielgruppengerecht informiert werden.

Ganz wichtig: Allein ein paar Bilder zur Illustration einer Kurzinformation zur Datenverarbeitung garantieren noch keine vorbildliche Umsetzung der Informationspflicht, wie dies in der DSGVO gefordert ist. Hier sei zur weiteren Lektüre auf die „Leitlinien für Transparenz gemäß der Verordnung 2016/679" (WP 260 rev.01) der Artikel-29-Datenschutzgruppe hingewiesen.[6] Speziell zum Textverständnis hilft zumindest für die deutsche Sprache der Hohenheimer Verständlichkeitsindex[7] weiter, der als Klartext-Initiative seine Praxistauglichkeit beispielsweise bei Versicherungspolicen unter Beweis gestellt hat. Zumindest kann nicht schaden, wenn der Verantwortliche die Anforderungen aus der Klartext-Checkliste[8] berücksichtigt, damit interessierte Personen die wichtigen Aspekte der Datenverarbeitung und ihrer Datenschutzrechte wirklich verstehen.

Über die Autorinnen

Marit Hansen
Landesbeauftragte für Datenschutz Schleswig-Holstein, Leiterin des ULD

Angelika Martin
Mitarbeiterin im Technikbereich des Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

▶ www.datenschutzzentrum.de

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Anzeige

Datenschutz im Fokus.

ZD – Zeitschrift für Datenschutz

9. Jahrgang 2019. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 259,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des
beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 199,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebs-/Direktbeorderungsgebühren (€ 14,20/€ 5,–) € 19,20 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. | 158812
facebook.com/verlagCHBECK LinkedIn.com/company/Verlag-C-H-Beck twitter.com/CHBECKRecht

C.H.BECK

WIE KANN MAN SECURITY AWARENESS MESSEN UND TRAINIEREN? – EINBLICK IN DEN »FAKTOR MENSCH« IN DER IT-SICHERHEIT

Anjuli Franz

Das Thema Awareness hält Einzug in Unternehmen und Behörden – IT-Sicherheitsverantwortliche realisieren, dass trotz technischer Schutzmaßnahmen echte Sicherheit ohne das Einbeziehen des Nutzers nicht möglich ist. Die Planung von Maßnahmen zur Steigerung des Sicherheitsbewusstseins birgt jedoch zahlreiche Herausforderungen. Wie kann Awareness gemessen und effektiv trainiert werden? Dieser Beitrag stellt eine Kennzahl vor und präsentiert Echtdaten aus über 60 europäischen Unternehmen.

Social Engineering: Der Nutzer als Einfallstor

Cyberkriminelle setzen vermehrt auf Social Engineering als Angriffsvektor – und denken sich dabei immer perfidere Taktiken aus. Social Engineering bezeichnet Angriffsmuster, die gezielt den Nutzer als Schwachstelle ausnutzen, um Zugriff auf Systeme zu erhalten oder Schadsoftware einzuschleusen. Enthielten im Jahr 2013 noch 17% aller Cyberangriffe eine Social Engineering-Komponente, so waren es im Jahr 2018 schon 35%[1], Tendenz steigend. Die Schadsoftware Emotet zeigt, welche Ausmaße diese Angriffe annehmen können. Als polymorpher Virus ist sie in der Lage sich bei jedem Abruf leicht zu verändern und so herkömmliche Antivirenprodukte zu täuschen. Sie verbreitet sich rasant über Spam-E-Mails, die immer schwieriger zu erkennen sind: Emotet liest gezielt Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus und nutzt diese Informationen zur weiteren Verbreitung. Der Empfänger wird so zum unbedachten Öffnen eines schädlichen Dateianhangs oder Links verleitet. Dieses Vorgehen von Emotet hat 2019 bereits zu zahlreichen Infektionen bei Unternehmen und Behörden geführt.[2]

Security Awareness stärkt die »menschliche Firewall«

Der Faktor Mensch sollte daher im Fokus der Sicherheitsmaßen stehen – das Schlagwort heißt »Security Awareness«. Security Awareness beschreibt das Ausmaß, in dem Mitarbeiter die Bedeutung von Informationssicherheit in ihrem Unternehmen sowie die Tragweite ihrer eigenen Sicherheitsverantwortlichkeit verstehen und dementsprechend handeln.[3] Gerade bei einer schwierig zu messenden Größe (wie quantifiziert man die Abwesenheit von Sicherheitsvorfällen?) stellen sich hier gleich mehrere Fragen, zum Beispiel:

- Wie stellt man sicher, dass Maßnahmen zur Security Awareness effektiv und nachhaltig sind?
- Kann ein Return on Investment angegeben werden? Lohnt sich die Investition?
- Gibt es einen Benchmark oder Vergleich mit anderen Organisationen ähnlicher Banchen?

Um das Thema Messbarkeit anzugehen, wurden bisher hauptsächlich Umfragen genutzt. Diese geben einerseits einen mehrdimensionalen Einblick in den Bereich Security Awareness aus Sicht der Mitarbeiter, leiden andererseits unter mangelnder Aussagekräftigkeit – Intention, angestrebtes und tatsächliches Verhalten klaffen oft weit auseinander. Ein weiterer Ansatz ist die Simulation einzelner Social Engineering-Angriffe, beispielsweise in Form einer Phishing-E-Mail. Bei einem solchen »Social Engineering-Penetrationstest« kann das Verhalten einer Testgruppe realitätsnah gemessen werden. Wie sieht es jedoch mit der Reproduzierbarkeit und Vergleichbarkeit des Messszenarios aus?

Um diese Probleme zu adressieren haben die Autoren eine neue Messmethode entwickelt, um die Security Awareness von Mitarbeitern standardisiert zu messen.

Klassifizierung von Angriffen als Grundlage für standardisierte Messmethode

Um Social Engineering-Angriffe miteinander vergleichbar zu machen, nehmen wir eine Klassifizierung in verschiedene Kategorien vor. Ausschlaggebend ist dabei die Vorbereitungszeit, die ein Krimineller in die Vorbereitung und Durchführung eines Angriffsszenarios investieren muss.

Kategorie	Zeitaufwand	Beispiel
1	ca. 1h	Wenig vorbereitete E-Mail in Unternehmenssprache.
2	ca. 3h	Mäßig vorbereitete E-Mail mit persönlicher Ansprache und Verwendung weniger Informationen.
3	ca. 10h	Angreifer übernimmt in E-Mail Rolle eines Kollegen oder Vertrauten der Testperson.
4	ca. 20h	E-Mail mit persönlichem Bezug, individuell vorbereiteter Telefonanruf oder einfacher physischer Angriff.
5	ca. 40h	Komplexer, mehrstufiger Angriff über verschiedene Ebenen.

Abb. 1: Klassifikation von Social Engineering-Angriffen nach aufzuwendender Vorbereitungszeit.

Diese setzt sich aus verschiedensten Faktoren zusammen, wie z.B. der Informationsbeschaffung (OSINT), der technischen Vorbereitung, dem Kopieren von Designs oder Login-Seiten (Clone Phishing), sowie der Ideenausarbeitung und Bereithaltung der Infrastruktur. So lassen sich fünf Kategorien einteilen, welche jeweils einer Vorbereitungszeit von ca. 1, 4, 10, 20 und 40 Stunden entsprechen.

Kennzahl für Security Awareness: Der Employee Security Index

Um die Awareness einer Testgruppe zu messen, wird nun jeder teilnehmende Mitarbeiter zum Ziel zufällig ausgewählter Angriffsszenarien verschiedener Kategorien. Sowohl einmalige Bestandsaufnahmen, beispielsweise eine Angriffssimulation über vier Wochen, in der jeder Teilnehmer zum Ziel von 2–3 Angriffsszenarien wird, als auch eine kontinuierliches Monitoring der Awareness sind möglich. Für alle Kategorien wird über die Testgruppe hinweg die »Erfolgs«rate gemessen.

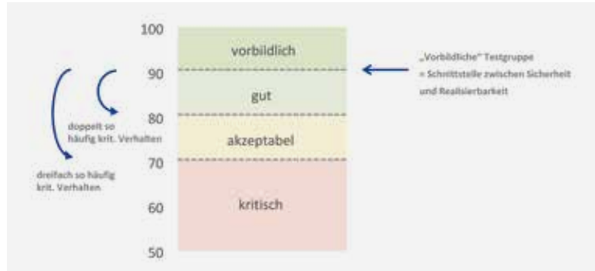


Abb. 2: Klassifikation von Social Engineering-Angriffen nach aufzuwendender Vorbereitungszeit.

Nun ist es utopisch, als angestrebtes Ziel eine Erfolgsrate von 0 zu setzen – Menschen machen Fehler. Wir definieren deshalb eine »vorbildliche« Testgruppe, welche an der Schnittstelle zwischen Sicherheit und Realisierbarkeit liegt. Abhängig von der Vorbereitungszeit, die ein Krimineller in den Angriff steckt, definieren wir Toleranzwerte, welches Verhalten noch als vorbildlich gewertet werden kann. Für die Social Engineering-Kategorien 1-3 liegen diese Toleranzwerte zwischen 1,5–6,5%. Eine vorbildliche Testgruppe mit exakt diesen Erfolgsraten erreicht auf der Skala einen Wert von 90. Wird doppelt (dreifach) so häufig kritisches Verhalten gezeigt, erreicht die Gruppe einen Wert von 80 (70). Ergebnisse unter 70 werden als kritisch bewertet (siehe Abbildung 2). Die Toleranzwerte basieren dabei auf der Erfahrung, welches Sicherheitsverhalten nach mehrmonatigen Awareness-Trainings erreicht werden kann. ▶

[1] 2019 Data Breach Investigations Record, Verizon.

[2] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

[3] Information Security Forum: »ISF Standard of Good Practice 2007«, CB3.4.

Durchführung von Awareness-Tests am Beispiel Phishing

Mit Hilfe der vorgestellten Methode wurde die Awareness gegenüber Phishing-Angriffen in über 60 europäischen Unternehmen und Behörden untersucht. Dabei wurden Phishing-Angriffe der Kategorien 1 bis 3 (d.h. eine bis zehn Stunden Vorbereitungszeit) simuliert, und die Klickrate auf Links und Dateianhänge gemessen. Beispiele für die simulierten Angriffe sind eine angebliche Meldung des Postfachs, der Speicher sei voll (Kategorie 1), die E-Mail eines zufälligen Kollegen, der einen Link zu einem lustigen GIF sendet (Kategorie 2), oder die Nachfrage eines bekannten Kollegen aus der gleichen Abteilung zu einem Hobby des Empfängers (Kategorie 3). Verwendet wurden hierbei Informationen, die vom Unternehmen selbst zur Verfügung gestellt wurden, sowie öffentlich verfügbare Informationen aus sozialen Netzwerken.

Insgesamt wurden über 75.000 E-Mails versendet, und die Ergebnisse auf Gruppenbasis mit einer Mindestgruppengröße von 30 Personen ausgewertet. In allen Fällen wurden die Teilnehmer vorher über das Durchführen einer Phishing Awareness-Maßnahme aufgeklärt, beispielsweise per Rundmail. Jeder Teilnehmer erhielt während der vierwöchigen Testphase 2-3 E-Mails individuellen Inhalts zu zufälligen Zeitpunkten.

Unternehmensübergreifender Einblick in Phishing Awareness

Abbildung 3 zeigt die Ergebnisse einer vierwöchigen Messung für einzelne Fachbereiche: Alle Testgruppen zeigen eine kritische Phishing Awareness, mit einem durchschnittlichen Employee Security Index von 46,2. Während die Abteilungen HR, IT und Finanzen unternehmensübergreifend überdurchschnittlich abschneiden, fallen am unteren Ende vor allem die Führungskräfte und das C-Level auf.

Nach dem vierwöchigen Test wurde für einige Testgruppen die Phishing-Simulation als kontinuierliches Awareness-Training über mehrere Monate durchgeführt. Hierbei wurden die Teilnehmer über einen »Teachable moment« über ihr Fehlverhalten aufgeklärt: Bei kritischem Verhalten wie dem Öffnen eines Links oder Dateianhang wurde der Nutzer auf eine Erklärseite weitergleitet, wo am Beispiel der eben erhaltenen E-Mail anschaulich aufgezeigt wurde, wie diese als Phishing hätte enttarnt werden können. Wie in Abbildung 4 dargestellt, konnten sich die Teilnehmer während dieser Maßnahme erheblich verbessern, und erreichten nach 8 Monaten im Durchschnitt (blau) einen Employee Security Index von 90. Auch bei den zunächst schwächeren Führungskräften (rot) ist eine Steigerung zu verzeichnen. Besonders in der Gruppe der Auszubildenden (lila) scheint bereits eine kurze »Starthilfe« zu genügen, um dauerhaft ein gesteigertes Bewusstsein für Phishing-E-Mails zu schaffen.

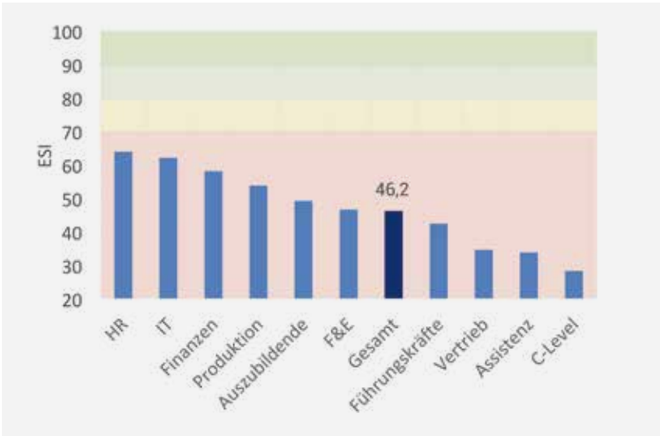


Abb. 3: Ermittlung des Employee Security Index im Rahmen einer vierwöchigen Phishing-Simulation für verschiedene Fachbereiche.

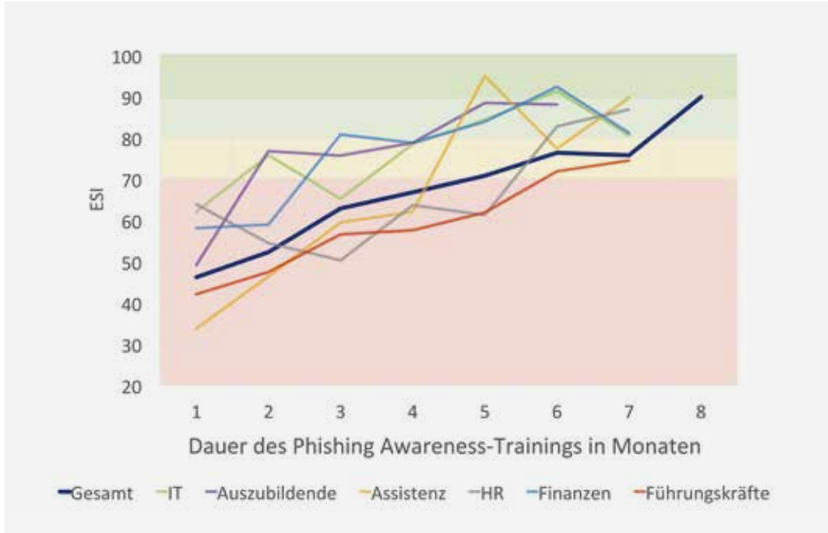


Abb. 4: Entwicklung der Phishing Awareness unterschiedlicher Fachbereiche während eines kontinuierlichen Awarenss-Trainings im Rahmen einer Phishing-Simulation. Die Daten sind unternehmensübergreifend.

Erweiterung des Konzepts: ganzheitliche Kennzahl

Um das Thema Security Awareness ganzheitlich abzubilden, können in den Employee Security Index neben Phishing Awareness weitere Faktoren eingebunden werden. Denkbar sind hier beispielsweise andere Angriffsvektoren wie Vishing (Telefon-Phishing) oder der Umgang mit gefälschten Login-Seiten. Das Melden von Vorfällen an die IT kann hingegen positiv eingerechnet werden. Auch Analysen zur Passwortkultur können in die Kennzahl einfließen. Daneben können regelmäßige Umfragen einen Einblick in die Motivation und Intention der Mitarbeiter geben.

Um auf die anfänglich gestellten Fragen zurück zu kommen:

Ein solcher Index stellt damit ein Kontrollinstrument dar, mit dem die Security Awareness in Unternehmen kontinuierlich überwacht werden kann. Die Effektivität von Schulungsmaßnahmen kann überprüft und der konkrete Bedarf einzelner Mitarbeitergruppen festgestellt werden. Die anonymisierte Auswertung der Ergebnisse auf Gruppenbasis trägt dabei dem Mitarbeiterschutz zu. Die Kommunikation sowohl mit dem Management als auch mit der Belegschaft wird durch eine greifbare Kennzahl erleichtert: Eine quantitative Analyse der Security Awareness bietet einen direkten Vergleich mit anderen Unternehmen ähnlicher Branchen und kann so als Entscheidungsgrundlage für weitere Investitionen genutzt werden.

Die regelmäßige Durchführung einer Awareness-Messung lässt die Themen Social Engineering und IT-Sicherheit zum festen Teil der Unternehmenskultur werden und steigert bei jedem einzelnen Mitarbeiter das Bewusstsein dafür, welche Verantwortung er als Anwender trägt.

Über die Autorin

Anjuli Franz
Ist ursprünglich Physikerin und seit eineinhalb Jahren bei IT-Seal als IT-Security Consultant tätig. Gemeinsam mit IT-Sicherheitsverantwortlichen europäischer Unternehmen und Behörden führt sie Projekte zur Security Awareness durch. Das Konzept des Employee Security Index findet Anwendung in der Kennzahl »ESI« von IT-Seal.

▶ anjuli.franz@it-seal.de

AUS DEM VERBAND

30 JAHRE
BERUFSVERBAND DER DATENSCHUTZBEAUFTRAGTEN DEUTSCHLANDS (BVD) e.V.

30 JAHRE BVD – FÜNF FRAGEN AN...

Frederick Richter

Vorstand der Stiftung Datenschutz

BvD-News: 1989 war das Jahr des deutschen und europäischen Aufbruchs – und der Gründung des BvD. Wie war es Ihrer Erinnerung nach damals um den Datenschutz bestellt?

Frederick Richter: Meine Erinnerung an den Zustand des Datenschutzes im Gründungsjahr ist leider alles andere als belastbar. Ich besuchte die 7. Klasse meines Gymnasiums, und der Datenschutz spielte thematisch mutmaßlich eine untergeordnete Rolle.

BvD-News: Was war für Sie das größte Ereignis in Sachen Datenschutz in den vergangenen Jahren?

Frederick Richter: Nun, ich dürfte nicht der einzige Interviewte sein, der hier die EU-Datenschutzgrundverordnung nennt...

BvD-News: Welche Initiativen des BvD sind Ihnen besonders in Erinnerung geblieben?

Frederick Richter: Da wir uns mit der Stiftung Datenschutz als Schirmherrin von Aktionstagen in Berlin eingebracht haben und auch ich selber vereinzelt mitwirkte, ist mir die Initiative „Datenschutz geht zur Schule" in guter Erinnerung geblieben. „Erinnerung" ist an dieser Stelle fast schon das falsche Wort, denn diese sehr löbliche Initiative lebt ja weiter. Freuen würde es mich dabei übrigens, wenn nicht nur die vielen ehrenamtlichen Unterstützerinnen und Unterstützer weiterhin mitmachen, sondern auch die öffentliche Hand einmal eine Förderung für „DSgzS" erwägen würde.

BvD-News: Welche Bedeutung hat der betriebliche Datenschutzbeauftragte, welche der BvD als Berufsverband Ihrer Einschätzung nach heute?

Frederich Richter: Betriebliche Beauftragte sind aus meiner Sicht eine unverzichtbare Ergänzung der Konstellation „Verantwortliche Stelle-Aufsichtsbehörde-Belegschaft". Sie können vermitteln und beraten, bevor es zu Auseinandersetzungen mit öffentlichen Stellen kommt. Sie sparen dem Unternehmen Kosten, denn die dauerhaft verfügbare Expertise interner oder externer DSB muss nicht kostenträchtig bei der Anwaltschaft eingekauft werden. Sie sind bestenfalls der ideale Transmissionsriemen, um Datenschutzaspekte so früh als möglich in die Entwicklung von Prozessen oder Produkten einfließen zu lassen. Mit ihrer Einbindung kann verhindert werden, dass es am Ende heißt: „geht nicht, wegen Datenschutz".

Die Politik ist aus meiner Sicht gut beraten, die bewährte Institution des betrieblichen Datenschutzbeauftragten nicht aufzuweichen und die Bestellpflicht einzuschränken. Zwar geht Deutschland an dieser Stelle, wie bereits vor der DSGVO über europäische Vorgaben hinaus. Doch haben wir dieses Modell von Selbstregulierung aus guten Gründen. Auch wirtschaftlich lohnt es sich. Denn eine frühe Warnung des eigenen Beauftragten kann davor schützen, mit datentechnisch riskanten Geschäftsmodellen womöglich in Sanktionsverfahren zu laufen, die am Ende teurer sind als Ressourcen für den DSB.

BvD-News: Was wünschen Sie dem BvD für die nächsten 30 Jahre?

Frederick Richter: Für den Zeitraum bis 2049 wünsche ich dem BvD, dass er zu allen kommenden Herausforderungen für Datenschutzbeauftragte den richtigen Rat geben kann.

Jan Philipp Albrecht

Minister für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung von Schleswig-Holstein. Zuvor hatte der Grünen-Politiker als Berichterstatter des Rechtsausschusses im EU-Parlament maßgeblich die Datenschutz-Grundverordnung ausgehandelt.

BvD-News: Was war für Sie die wegweisendste Entwicklung beim Datenschutz in den vergangenen Jahren?

Jan Philipp Albrecht: Das Bewusstsein über die Notwendigkeit von Datenschutz ist mittlerweile in der Gesellschaft angekommen. Mit der Digitalisierung weiterer Bereiche der Wirtschaft und datengetriebener neuer Geschäftsmodelle entstehen Probleme, die hochkomplex und vernetzt sind. Gleichzeitig erheben die Bürgerinnen und Bürger die berechtigte Forderung nach einer modernen und digitalen öffentlichen Verwaltung, welche die Daten zum Wohle der Menschen einsetzt oder bereitstellt. Die Diskussion um „Daten als neues Öl" ist ein Gradmesser dieser Entwicklung. Digitale Tools sind tief mit dem normalen Alltag der Menschen verwoben und werden wie selbstverständlich auch unter Datenschutz-Gesichtspunkten betrachtet.

Das müssen wir politikseitig fördern und stärken. Deswegen haben wir in Schleswig-Holstein in unserem Digitalisierungsprogramm explizit die Förderung des transparenten, evidenzbasierten Regierungshandelns verankert.

BvD-News: Welche Rolle hat Ihrer Einschätzung nach der betriebliche Datenschutzbeauftragte – auch als teils neue Institution im europäischen Kontext?

Jan Philipp Albrecht: Datenverarbeitung ist so vielfältig, dass sie nicht von einer zentralen Stelle wie den Aufsichtsbehörden beobachtet und kontrolliert werden kann. IT-Systeme werden in immer kürzeren Zeitabschnitten entwickelt, getestet und implementiert. In jeder Anwendung und jedem Prozess entstehen dabei lokale Besonderheiten, die lokales Wissen erfordern. Datenschutzbeauftragte sind daher unverzichtbare Kontrollinstanzen vor Ort. Dieses Modell war in Deutschland erfolgreich und gilt jetzt mit der DSGVO für die ganze EU. Hier gilt es in einen gegenseitigen Erfahrungsaustausch zu treten und auch von unseren europäischen Partnern zu lernen, die den dezentralen Datenschutz vielleicht mit einer neuen Perspektive angehen.

BvD-News: Welche Relevanz hat Ihrer Erfahrung nach der Berufsverband für Datenschutzbeauftragte? Wie bewerten Sie die Frage nach einer Berufskammer für Datenschutzbeauftragte?

Auch wenn das Wissen zur Kontrolle vor Ort stark dezentralisiert ist, fließt es doch immer wieder an bestimmten Punkten in übergeordneten rechtlichen Normen und Standardisierungen zusammen. Bei einer sich schnell entwickelnden technischen Umgebung und einem raschen rechtlichen Wandel kann es hier für den Einzelnen schwer sein, den Überblick zu behalten. Der Berufsverband für Datenschutzbeauftragte ist hier ein unverzichtbares Forum, um zu gemeinsamen Ideen und Stellungnahmen zu kommen. Gleichzeitig ist der Berufsverband ein Sprachrohr, um die besondere Perspektive der Datenschutzbeauftragten zwischen Aufsichtsbehörden und Verantwortlichen zu artikulieren. Die Umwandlung in eine Berufskammer könnte diesen Herausforderungen noch effektiver begegnen. Zum Beispiel könnte eine solche Berufskammer verbindlich formulieren, was es eigentlich heißt, dass die Datenschutzbeauftragten das „erforderliche Fachwissen" haben. Dabei läge die Schwierigkeit sicherlich darin, in einer Kammer das komplette Feld der sehr heterogenen Datenschutzbeauftragten-Landschaft abzubilden. Die Palette reicht immerhin vom Datenschutzbeauftragten im Fußballverein bis zur Datenschutzbeauftragten im Großkonzern.

BvD-News: Was wünschen Sie dem BvD für die nächsten 30 Jahre?

Ich wünsche mir einen starken BvD, der seinen Informationsauftrag gegenüber allen interessierten Bürgerinnen und Bürgern weiterhin so ernst nimmt wie bisher und zudem noch mehr als Hafen und Anlaufstelle für Datenschutzbeauftragte in Erscheinung tritt. Wissen über Datenschutz sollte mit möglichst wenig Zugangsbarrieren so verständlich und anwenderbezogen wie möglich vermittelt werden. Das Datenschutz-Wiki (www.datenschutz-wiki.de) ist ein guter Schritt in diese Richtung. Warum nicht auch Online-Seminare oder Datenschutz-Tools wagen, wie es die französische und bayerische Aufsichtsbehörde mit PIA versucht? Jetzt wird es darum gehen, mit der Zivilgesellschaft und anderen Datenschützern in ganz Europa in einen Austausch zu treten. Der BvD wird dabei hoffentlich weiterhin sowohl Motor als auch Koordinator dieses Austausches sein.

AUS DEM VERBAND

Prof. Dr. Armin Herb

Rundfunkbeauftragter für den Datenschutz beim SWR, und Ehrenmitglied des BvD

BvD-News: 1989 war das Jahr des deutschen und europäischen Aufbruchs - und der Gründung des BvD. Wie war es Ihrer Erinnerung nach damals um den Datenschutz bestellt?

Armin Herb: 1989 war auch das Datenschutzrecht im Aufbruch und Umbruch. Seit dem Volkszählungsurteil vom Dezember 1983 waren inzwischen mehr als fünf Jahre vergangen und nach langen Mühen wurde dann im April 1989 ein Regierungsentwurf zur Fortentwicklung der Datenverarbeitung und des Datenschutzes in den Bundestag eingebracht. Parallel waren und wurden auf der Basis des Volkszählungsurteils neue Landesdatenschutzgesetze erlassen. Die Gesellschaft für Datenschutz und Datensicherheit (GDD) propagierte jedoch einen Datenschutz mit Augenmaß und die Deutsche Vereinigung für Datenschutz (DVD) verstand sich als kritisches Bürgerrechtsforum. Der Datenschutzbeauftragte führte ein Schattendasein und war damals ohne Interessenvertretung. Um sowohl den Datenschutz als Schutz des Persönlichkeitsrechts des Einzelnen als auch die Institution des Datenschutzbeauftragten zu fördern, wurde der BvD gegründet. Zunächst mit dem Namen Bundesverband und dann, nach anwaltlichem Vorgehen der GDD, in Berufsverband umbenannt.

BvD-News: Was war für Sie das größte Ereignis in Sachen Datenschutz in den vergangenen Jahren?

Armin Herb: Betrachtet man die Geschichte des Datenschutzes seit dem ersten Bundesdatenschutzgesetz von 1977 so gibt es in meinen Augen zwei wichtige Ereignisse: Das eine ist das legendäre Volkszählungsurteil und das andere ist jetzt die Europäische Datenschutz-Grundverordnung (DSGVO).

BvD-News: Welche Initiativen des BvD sind Ihnen besonders in Erinnerung geblieben?

Armin Herb: Der BvD hat in der Vergangenheit und auch heute noch eine Vielzahl von Initiativen nicht nur zur Förderung des Datenschutzes, sondern auch zur Stärkung des Datenschutzbeauftragten auf den Weg gebracht. Die schönste Initiative für mich war die rasche Umsetzung und Einführung des von mir vorgeschlagenen Datenschutz-Medienpreises DAME.

BvD-News: Welche Bedeutung hat der betriebliche Datenschutzbeauftragte, welche der BvD als Berufsverband Ihrer Einschätzung nach heute?

Armin Herb: Die erstmalige Bestellungspflicht für betriebliche Datenschutzbeauftragte bestand zum 1. Juli 1978. Seitdem sind über 40 Jahre vergangen. Im Laufe dieser Zeit war die Bedeutung, das Image und die Wahrnehmung der Datenschutzbeauftragten in der Öffentlichkeit von Höhen und Tiefen bestimmt. Aber trotz mancher Rückschläge haben die Datenschutzbeauftragten heute eine nie da gewesene Bedeutung. Auch der BvD hat sich gerade in den letzten Jahren rasant entwickelt. Damit einhergehend haben auch andere Institutionen ihr Herz für den Datenschutzbeauftragten entdeckt. Der BvD ist heute eine nicht mehr weg zu denkende Institution für den Datenschutz und die Datenschutzbeauftragten.

BvD-News: Was wünschen Sie dem BvD für die nächsten 30 Jahre?

Armin Herb: Ich hoffe und wünsche, dass der BvD sich kontinuierlich weiterentwickelt; langsam, aber stetig. Er sollte nicht nur Interessenvertretung von Datenschutzbeauftragten sein, sondern auch Sprachrohr für den Datenschutz. Und wenn sich einmal der Wind dreht und der Datenschutz vorübergehend zurückgedrängt wird, so wünsche ich dem BvD die Kraft, dass er diese Durststrecken durchhält.

Prof. Dr. Thomas Petri

Bayerischer Landesbeauftragte für den Datenschutz

BvD-News: 1989 war das Jahr des deutschen und europäischen Aufbruchs - und der Gründung des BvD. Wie war es Ihrer Erinnerung nach damals um den Datenschutz bestellt?

Thomas Petri: Der Beginn meiner persönlichen Auseinandersetzung mit dem Datenschutz fällt zeitlich fast mit der Gründung des BvD zusammen. 1987 gab es ja die zweite Volkszählung, 1989 das zweite Schengener Abkommen, dass das erste Abkommen von 1985 umsetzen sollte. Dadurch wurden die innereuropäischen Grenzen abgeschafft, die Grenzkontrollen an den EU-Außengrenzen aber verstärkt. Dazu wurde ein EU-weites Informationssystem installiert. Bei uns wuchs damals die Sorge, dass durch die gemeinsame Polizeiarbeit mit anderen Ländern der Ausverkauf des relativ hohen deutschen Datenschutz-Niveaus stattfinden wird.

Schon damals sagte mein Rechtslehrer Professor Spiros Simitis, der ja auch Datenschutzbeauftragter von Hessen war, Datenschutz werde zum Prüfstein, wie ernst es die Politiker mit dem Europa der Bürger wirklich meinen. Uns war klar, dass man den Datenschutz stärken und in Position bringen muss.

BvD-News: Welche Initiativen des BvD sind Ihnen besonders in Erinnerung?

Thomas Petri: Schon relativ früh hatte ich mit dem BvD zu tun. Im Unterschied zur GDD erschien mir der BvD schon damals als der politisch aktivere Verband. Seine Haltung, dass die Betriebe den Datenschutz mitdenken müssen, gefiel mir. Ebenso das Engagement des Verbands in den vergangenen Jahren für den betrieblichen Datenschutzbeauftragten, auch im europäischen Gesetzgebungsprozess.

Wenn ein Verband, dessen Mitglieder und Vorstände aus der Praxis kommen, betont, dass ein Datenschutzbeauftragter keine bürokratische Hürde, sondern eine Stärkung der Demokratie bedeutet, dann finde ich das sehr überzeugend. Auch hat der BvD sehr aktiv gegen die Versuche, die Benennungspflicht von betrieblichen DSB zu lockern, interveniert.

BvD-News: Welche Bedeutung hat der betriebliche Datenschutzbeauftragte, welche der BvD als Berufsverband Ihrer Einschätzung nach heute?

Thomas Petri: Ich selbst bin ein Befürworter der sogenannten regulierten Selbstregulierung, wofür die betrieblichen Datenschutzbeauftragten stehen. Auch sind sie wichtige Ansprechpartner für uns Aufsichtsbehörden und haben sich als Institution absolut bewährt.

BvD-News: Was wünschen Sie dem BvD für die nächsten 30 Jahre?

Thomas Petri: Die größte Herausforderung sehe ich in den weiteren europäischen Abstimmungen etwa zur ePrivacyVerordnung. Das Projekt Datenschutz ist auf europäischer Ebene noch nicht zu Ende. Deshalb wünsche ich dem BvD, dass er genau so weitermacht, wie bisher, dass seine Bedeutung in Wirtschaft und Gesellschaft noch zunimmt.

Riko Pieper

Stellvertretender Sprecher der BvD-Initiative „Datenschutz geht zur Schule“ und Vize-Vorstand der Deutschen Vereinigung für Datenschutz (DVD)

BvD-News: 1989 war das Jahr des deutschen und europäischen Aufbruchs – und der Gründung des BvD. Wie war es Ihrer Erinnerung nach damals um den Datenschutz bestellt?

Riko Piper: Ich war von 1984 bis 1990 in Argentinien und habe den Mauerfall nur aus der Ferne erlebt. Zwar habe ich noch das Volkszählungsurteil im Dezember 1983 mitkommen, aber aktiv im Datenschutz war ich noch nicht. Seit 1993 war ich bei der deutschen Flugsicherung - erst im QM, dann in IT-Revision und Datenschutz - tätig.

BvD-News: Was war für Sie das größte Ereignis in Sachen Datenschutz in den vergangenen Jahren?

Riko Pieper: Ein einschneidendes Erlebnis war für mich der Bahn-Skandal, der 2009 bekannt wurde. Danach hatte die Deutsche Bahn über Jahre 175.000 Mitarbeiter ausgespäht, um Korruption zu bekämpfen – und dabei Namen, Anschriften und auch Kontodaten der Mitarbeiter abgeglichen.

Nachdrücklich beeinflusst hat mich aber auch die NSA-Affäre, die der frühere CIA-Mitarbeiter Edward Snowden mit der Veröffentlichung der PRISM-Dokumente 2013 lostrat. In der Folge machte sich Europa auf den Weg, ein neues Datenschutzgesetz zu erlassen, was 2016 in die Datenschutz-Grundverordnung mündete.

BvD-News: Welche Initiativen des BvD sind Ihnen besonders in Erinnerung geblieben?

Riko Pieper: Ich bin ja stellvertretender Sprecher der BvD-Initiative „Datenschutz geht zur Schule“. Die ist nicht nur für die Datenschutz-Bildung wichtig, sondern auch für mich persönlich. Ich glaube auch, dass die Initiative für den Verband ein Türöffner in die Politik war. Mittlerweile kommen auf die Verbandstage viele interessante Leute aus Politik und Wirtschaft. Das war vor der Initiative schwieriger. Mit den Schülerinnen und Schülern, die wir im Laufe der Zeit erreicht haben, könnten man mittlerweile ein ganzes Fußballstadion füllen.

BvD-News: Welche Bedeutung hat der betriebliche Datenschutzbeauftragte, welche der BvD als Berufsverband Ihrer Einschätzung nach heute?

Riko Pieper: Die Anfragen an die DSB sind über die Jahre viel zahlreicher geworden, natürlich in erster Linie auch durch die DSGVO. Dadurch ist Datenschutz mittlerweile in den Köpfen der Bürgerinnen und Bürger angekommen. Entsprechend gibt es immer mehr konkretere Anfragen – und zwar von Unternehmen und von Bürgern. Damit steigt der Bedarf und die Verantwortung der Datenschutzbeauftragten.

Das zeigt sich auch im Selbstverständnis des BvD. Der in Kooperation mit der Gesellschaft für Datenschutz und Datensicherheit (GDD) entwickelte Standard für ▸

Datenschutzbeauftragte und die Vereinfachung des Audit-Prozesses war ein wichtiger Schritt hin zur ersten Adresse als Berufsverband. Das Auftragsverarbeitungs-Audit gehörte vorher nicht zu den Aufgaben des BvD.

Im Diskurs mit der Politik ist vor allem der amtierende Vorstand sehr engagiert. Er hat sich zuletzt dafür stark gemacht, dass die aktuelle Benennungspflicht für Datenschutzbeauftragte erhalten bleibt – im europäischen Kontext und in Deutschland.

BvD-News: Was wünschen Sie dem BvD für die nächsten 30 Jahre?

Riko Pieper: Weiterhin viel Erfolg.

Dr. Stefan Brink

Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg

BvD-News: Was war für Sie die größte bzw. wegweisendste Entwicklung beim Datenschutz in den vergangenen Jahren?

Stefan Brink: Neben der DSGVO war das für mich das Urteil des Europäischen Gerichtshofs zur Unabhängigkeit der Aufsichtsbehörden. Wir sind damit von den Innenbehörden unabhängig geworden. Das hat uns stärker gemacht. Der Pferdefuß dabei ist allerdings, dass die personelle Ausstattung der Aufsichtsbehörden den Aufgaben hinterherhinkt. Im Ganzen sehen ich das aber als eine sehr positive Entwicklung an.

BvD-News: Welche Initiativen des BvD sind Ihnen besonders in Erinnerung?

Stefan Brink: Zu allererst denke ich dabei an das Engagement des BvD zum Erhalt des Datenschutzbeauftragten, auch gegenüber dem Bundestag. Zum Erhalt der Benennungspflicht hat der BvD alle Kanäle genutzt. Aber auch „Datenschutz geht zur Schule“ ist eine tolle Initiative. Eine Reihe von Aufsichtsbehörden beteiligt sich mittlerweile daran, weil wir von dem Engagement, Datenschutz gerade jungen Leuten näher zu bringen, begeistert sind.

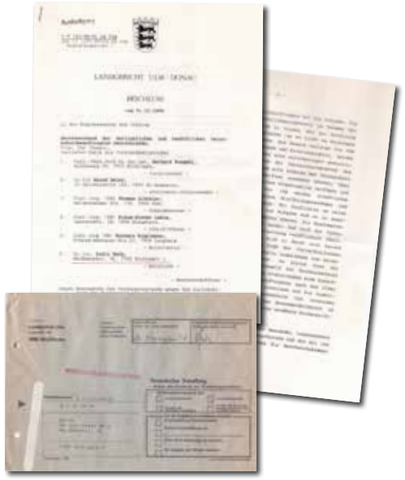
BvD-News: Welche Bedeutung hat Ihrer Einschätzung nach der betriebliche Datenschutzbeauftragte, welche der BvD als Berufsverband?

Stefan Brink: Grundsätzlich hat sich meiner Meinung nach die Rolle des Datenschutzbeauftragten gar nicht so sehr verändert. Er hat schon immer mehr als die Aufsichtsbehörden dafür gesorgt, dass es in Deutschland ein hohes Datenschutz-Niveau gibt. Das ist ja ganz entscheidend, dass mit der Institution des Datenschutzbeauftragten Leute in die Betriebe kommen, die sich wirklich auskennen.

Leider ist es nicht gelungen, dieses deutsche Modell verpflichtend für alle EU-Länder in der DSGVO festzuschreiben. Wir müssen also weiterhin auf EU-Ebene Überzeugungsarbeit leisten, wie wichtig Datenschutzbeauftragte auch für uns als Aufsichtsbehörden sind.

BvD-News: Was wünschen Sie dem BvD für die nächsten 30 Jahre?

Stefan Brink: Ich wünsche dem BvD, dass er seine starke Rolle als Fürsprecher der Datenschutzbeauftragten behält und sich weiterhin für ein hohes Datenschutz-Niveau einsetzt.



Die Entscheidung des Landgerichts Ulm zur Frage, ob der Datenschutzbeauftragte ein Beruf ist, ist von überragender Bedeutung für die Entwicklung des BvD und der Institution eines Datenschutzbeauftragten.

Original-Zustellungsurkunde zum Beschluss vom 31.10.1990, die erste Seite des Beschlusses sowie die entscheidende Seite 10 zeigt, in dem die Ausführungen zum Beruf des Datenschutzbeauftragten enthalten sind.

BvD-News – im Wandel der Zeit

Anzeige

DSGVO Praxis-workshops für Datenschutz-beauftragte.

Jetzt exklusive Praxis-Tipps sichern!

Seit Mai letzten Jahres ist die Anwendung der EU-DSGVO Pflicht. Dennoch gibt es in vielen Unternehmen noch große Unsicherheiten. Vor allem jetzt – wo die ersten schweren Strafen verhängt worden sind.

Sie kämpfen in Ihrem Arbeitsalltag auch noch mit der Umsetzung?
Wir bieten Ihnen einen Praxisworkshop, in dem es nur um praxisrelevante Inhalte und Fragen geht!

Ihre Vorteile im Überblick:

- Praktische Beispiele und Übungen stehen im Vordergrund und helfen Ihnen bei der Umsetzung der DSGVO.
- Sie können in den Erfahrungsaustausch mit anderen Teilnehmern und dem Dozenten gehen und Ihre ganz konkreten individuellen Fragen und Probleme klären.
- Durch reale Fallbeispiele arbeiten Sie datenschutzrelevante Themen durch und auf.
- Wir stellen Ihnen Vorlagen, Praxistipps und Handlungsempfehlungen zur Verfügung.

Weitere Infos und alle Termine finden Sie unter www.tuv.com/seminar-32118

Wir freuen uns auf Ihre Teilnahme!

PS: Unser gesamtes Datenschutzportfolio, inklusive aller Lehrgänge, neuer Seminare und Event-Ankündigungen finden Sie unter www.tuv.com/datenschutz

Sollten Sie vorab noch Fragen haben, stehen wir Ihnen gerne zur Verfügung.

Sandra Fahling
Business Managerin Datenschutz
Tel. 0221 – 806 3561
sandra.fahling@de.tuv.com

www.akademie.tuv.com

TÜVRheinland®
Genau. Richtig.

AUS DEM VERBAND

EUROPEAN FEDERATION OF DATA PROTECTION OFFICERS (EFDPO) IN BERLIN

Regina Mühlich, Thomas Spaeing

Mit der Verabschiedung der EU-DSGVO wurde die Basis für den einheitlichten Datenschutz in der EU geschaffen und mehr noch, ein Startsignal für die weltweite Neuorientierung im Datenschutz gegeben. Die Funktion des betrieblichen und behördlichen Datenschutzbeauftragten wurde damit erstmals in allen EU-Mitgliedsstaaten eingeführt. Im Zusammenhang mit der rasch voranschreitenden Digitalisierung und dem zunehmenden Einsatz von KI-Systemen nimmt auch die Bedeutung des Datenschutzes und insbesondere die des Datenschutzbeauftragten erheblich zu.

Um diesen Entwicklungen Rechnung zu tragen, hat der BvD bereits vor einem Jahr begonnen Gespräche mit potentiellen Partnerverbänden in der EU zu führen, die wie der BvD als Berufsverband die Interessen der im Datenschutz tätigen Personen vertreten und fördern. Ziel war dabei die Gründung eines unabhängigen Dachverbandes auf EU-Ebene. Das Berufsbild wird zunehmend aus Brüssel bestimmt und es gilt daher gerade dort die Gesamtinteressen dieser Berufsgruppen wahrzunehmen.

Nach Arbeitstreffen in Lissabon, Prag und Wien konnte der BvD mit sieben Partnerverbänden im Anschluss an die diesjährigen Verbandstage am 07. Juni 2019 den europäischen Dachverband der Datenschbeauftragten (EFDPO) gründen.

Gründungsmitglieder der European Federation of Data Protection Officers (EFDPO) sind neben dem BvD nationale Verbände für Datenschutzbeauftragte aus Österreich, Frankreich, Portugal, Tschechien, der Slowakei, Griechenland und Liechtenstein. Ziele der Neugründung sind u.a. die Datenschutzbeauftragten in den EU-Mitgliedsverbänden miteinander zu vernetzen und ihre Interessen in Brüssel zu vertreten. Dabei soll der Datenschutz als Wettbewerbs- und Standortvorteil für Europa gestärkt und weiterentwickelt werden. Der Verbandssitz liegt entsprechend des Auftrags in Brüssel.

Auch weitere Berufsverbände zu den im Datenschutz tätigen Personen können und sollen Mitgied in der Dachorganisation werden. Es sind auch mehrere Verbände eines Landes zugelassen. Für die weitere Erweiterung ist bereits vorgesorgt: Falls Länder ausserhalb der EU Mitglied werden möchten, können diese assoziierte Mitglieder werden und können sich an allen Aktivitäten im Interesse ihrer Mitglieder beteiligen. Neben diesen Mitgliedschaften besteht für Unternehmen und Organisationen auch die Möglichkeit, sich als Partner des EFDPO eintragen zu lassen und so von den Aktivitäten zu profitieren und diese zu unterstützen.

Es bestehen bereits erste inhaltliche Kontakte, die auch zu einer internationalen Vernetzung nah an der Praxis führen sollen. Die Arbeit des AK Medizin des BvD trifft hier beispielsweise auf breites Interesse bei den Mitgliedsverbänden. Normierungsbestebungen in anderen Ländern sind beispielhafte Erfahrungen, von denen wiederum der BvD profitieren kann. Der EU-Verband will sich unter anderem auch dafür einsetzen einen EU-Zertifizierungsstandard für Datenschutzbeauftragte zu etablieren. Der BvD kann nun also auch Kontakte in verschiedenen Mitgliedsstaaten vermitteln, die bei Fragen der europäischen Zusammenarbeit weiterhelfen können.

„Die EFDPO vereint die Stimmen der nationalen Datenschutzbeauftragten-Verbände zu einer starken Vertretung auf EU-Ebene“, sagte BvD-Vorstandsvorsitzender Thomas Spaeing.

Zu den formalen Schritten der Gründung gehört auch, dass das Logo (GRAFIK) als Unionsmarke Ende Juni 2019 beim Amt der Europäischen Union für geistiges Eigentum (EUIPO) registriert wurde. Die Domain (www.efdpo.eu) ist angemeldet und die Webseite wird in in Kürze mit ersten Informationen online gehen. Die Satzung ist konzeptionell durch die Gründungsmitglieder erstellt und „verabschiedet“ worden. Der BvD hatte in der letzten Mitgliederversammlung der aktiven Beteiligung in der EFDPO einstimmig zugestimmt. Aktuell wird die Satzung der EFDPO durch einen belgischen Anwalt geprüft und anschließend im belgischen Verbandsregister eingetragen. Die Arbeitssprache der EFDPO ist die englische Sprache.

Die einzelnen Mitgliedsverbände sind nun dabei sich so zu organisaieren, dass der EFDPO arbeitfähig wird. Dazu werden je Mitgliedsverband Ausschüsse bzw. Arbeitsgruppen gegründet, welche die Mitarbeit im europäischen Verband vorbereiten sollen. Diese Teams sollen auch grenzübergreifend zusammenarbeiten, um die Aufgaben voranzutreiben und bspw. gemeinsame Papiere für die Gremien in Brüssel zu erstellen, die dann die Arbeit der EFDPO flankieren. So sollen bspw. auch zu den geplanten Evaulierungen der DSGVO Standpunktpapiere aus Sicht des DPO und der weiteren im Datenschutz tätigen Funktionen verfasst werden.

Um die Arbeit des EU-Dachverbandes auf deutscher Seite voranzutreiben, wird der Ausschuss „EU-Aufgaben“ gegründet, an dem man sich aktiv beteiligen kann.

Der EU-Dachverband wird sich aktiv in Brüssel und in der EU zum Datenschutz und vor allem zum DSB einbringen. Der Ausschuss wird die wesentliche Arbeit dazu übernehmen und durch den Vorstand geleitet werden.

Die EU-Partnerverbände streben einen intensiven Erfa-Austausch und auch grenzübergreifende Arbeitsgruppen an. Die Mitglieder des Ausschusses unterstützen hier und nehmen in diesem Zusammenhang ggf. Termine bei/mit den EU-Partnerverbänden wahr.

Voraussetzungen zu Teilnahme sind englische Sprachkenntnisse in Wort und Schrift, gerne weitere Sprachkenntnisse, ggf. Reisebereitschaft.

Der Ausschuss „EU-Aufgaben“ wird sich mit den entsprechenden Themen und Strategien befassen, um hier Verbesserungen zu erarbeiten und den entsprechenden Stellen in der EU vorzuschlagen.

Mitglieder, die in dem Ausschuss mitarbeiten möchten, können sich via E-Mail unter bvd-gs@bvdnet.de bewerben.

Über die Autoren

Regina Mühlich
Mitglied im Vorstand des BvD

Thomas Spaeing
BvD-Vorstandsvorsitzender

v. l. n. r.
Pavol Szabo
Jürgen Hartz
Judith Leschanz
Vladan Rámiš
Inês Oliveira
Renate Riedl
Margarida Ferreira
Thomas Spaeing
Regina Mühlich
Xavier Leclerc
Philipp Mittelberger

DAME-GALA: MIT DER GLITTERKANONE AUF DIE GEWINNER

Zweiter Datenschutz Medienpreis bringt Rhythmus und Emotionen in die Verbandstage 2019

Dass Datenschutz Spaß machen kann, davon ist die Jury des Datenschutz Medienpreises zutiefst überzeugt. Denn auch bei der zweiten Vergabe der DAME auf den Verbandstagen 2019 in Berlin kürte die Jury kurzweilige, witzige und berührende Arbeiten, die damit genau ihre Zielgruppen treffen.

Den mit 3.000 Euro dotierten Hauptpreis holten die schweizer Multimedia-Studenten Meret Kaufmann, Gion Hunziker und Nicolas Zürcher mit einem Kurzfilm über Chancen und Risiken von Gesundheitsdaten. In dem Zukunftsszenario erzählen sie die Geschichte eines jungen Mannes, dessen Lebenslauf dank Fitness-App und Smart-Watch ins falsche Licht rückt.

Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands (vzbv) und Jury-Laudator betonte, dass er die Geschichte für gar nicht mehr so fiktiv halte. Er verwies auf Versicherungen, die schon heute Fitness- und Ernährungsgewohnheiten ihrer Mitglieder erfassten. „Variablen Beiträge, die den Lebenswandel bewerten, könnten auch in Deutschland bald Realität werden“, sagte er.

BvD-News: Wie entstand die Idee für die Geschichte?

Meret Kaufmann: Viele Leute wissen, was Big Data bedeutet und wie Daten dabei verwendet werden. Aber welche Auswirkungen das auf den Einzelnen hat, das können sich dann doch nur wenige vorstellen. Und das wollten wir zeigen.

Nicolas Zürcher: Wir haben dann das Thema ein bisschen zugespitzt und gezeigt, wie es sein könnte. Aber vielleicht sind wir gar nicht mehr so weit von der Realität entfernt.

Gion Hunziker: Wir zeigen eigentlich, wie es enden könnte, wenn die Leute sich nicht um ihre Daten kümmern und nicht darüber nachdenken, wo sie welche Daten hinterlassen. Es dürfte schon bald in Europa bei den Krankenkassen dynamische Preise geben. Für den Einzelnen dürfte es dann schwierig sein, sich gegen den Apparat zu stellen. Hier ist meiner Meinung nach der Staat gefragt. Er muss seine Bürger vor den Wirtschaftsinteressen von Konzernen schützen.

ZDF-Redakteurin Nadja Kronemeyer gewann in der Kategorie „Bestes Jugendangebot“ einen mit 1.500 Euro dotierten Preis für das von ihr verantwortete ZDF-Online-Angebot „App+On“ für Kinder und Jugendliche. Auf der Plattform spielt eine Gruppe von junge Laienschauspielern, die Kronemeyer zufolge auch im echten Leben befreundet sind, in Clips und Videos Szenen, in denen sie Kinder und Jugendliche für den Umgang mit Smartphones und Apps sensibilisieren, zugleich aber den Kindern Spaß vermitteln wollen. Jury-Laudatorin Steffi Rack von der Internet-Initiative klicksafe lobte die Plattform: „Die Videos bieten Lösungen an, da können wir auch noch etwas lernen“, sagte sie bei der Preisverleihung.

BvD-News: Welches Ziel verfolgten Sie mit „App+On“?

Ulrike Willner: Wir betrachten es als unsere Aufgabe, Kindern und Jugendlichen ein Angebot zu machen, das sie verstehen können. Dabei sagen wir ihnen: Habt Spaß online, aber seid vorsichtig.

Nadja Kronemeyer: Unsere Schauspieler, alles Laien und auch im echten Leben befreundet, wirken auf die Kinder, die unser Angebot nutzen, wie ältere Brüder oder Schwestern. Denen glauben sie mehr als uns Erwachsenen, wenn es zum Beispiel darum geht, was sie tun müssen, wenn sie ihr Smartphone verloren haben. Das sehen wir auch an den Kommentaren, die wir nur anonymisiert auf der Seite veröffentlichen. Ein bisschen sind die Darsteller und Clips wie eine kleine Soap für die Zielgruppe geworden. Manchmal bekommen wir Anfragen, in denen Kinder fragen, ob sie bei den Clips und Filmen mitspielen können.

Ulrike Willner: Das freut uns natürlich und zeigt uns, dass unser Angebot von der Zielgruppe als sehr authentisch wahrgenommen wir. Aber das geht leider nicht.

Der Song „Spiel mit offenen Daten“ von Alex Döring und der Videofilmerin Mona Feyrer holte die DAME 2018 in der Kategorie „Bester musikalischer Beitrag“ – und bekam dafür ebenfalls 1.500 Euro.

Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen, sprach der Song an, weil er originell sei, aber auch die Datenerfassung durch den Staat kritisch beleuchte, wie sie bei der Preisverleihung sagte.

Döring ist der zweite Musikbeitrag, der die sechsköpfige Jury aus Datenschutz- und Medienexperten begeisterte. Im vergangenen Jahr, beim ersten DAME-Wettbewerb, bekam Kevin Lehmann einen von klicksafe gestifteten Sonderpreis für seinen Rap „Datenschutz“. Die DATEV-Stiftung Zukunft und der BvD drehten mit ihm im Anschluss noch ein Video.

Die gleich dreifache Preisauszeichnung war der Begeisterung der Jury geschuldet, mit der sie bei der Preisverleihung das Publikum anstiftete. „Jurysitzungen können manchmal zäh sein“, sagte Verbraucherschützer Klaus Müller. Aber die Arbeit in der DAME-Jury sei für ihn wunderbar gewesen. „Das zeigt, wie spannend die Beiträge waren.“

BvD-News: Woher hatten Sie die Idee für den Song?

Alex Döring: Die Idee kam mir bereits 2015. Nachdem Edward Snowden die PRISM-Dokumente an die Öffentlichkeit gegeben hatte entstanden in der Folge Polizeigesetze, die auf eine Sammlung von Bürgerdaten abzielen. Gegen die Datensammelwut von Unternehmen haben wir die Datenschutz-Grundordnung. Aber gegen die staatliche Überwachung kann sich der Einzelne nicht wehren.

Mona Feyrer: Oft merken wir gar nicht, dass wir zu viele Daten preisgeben. Das fängt bei Angeboten wie Pay-Back-Werbeaktionen von Unternehmen an und geht bis hin zum Staat, der Daten von uns abgreift, ohne dass wir es merken.

Kinder und Jugendliche prägen morgen den Datenschutz

Für die Sichtung der Einreichungen musste die Jury in diesem Jahr mehr Zeit aufbringen, „denn da waren auch Beiträge mit einer Dauer von zwei Stunden dabei", wie BvD-Vorstandsvorsitzender Thomas Spaeing erzählte. Er führte an der Seite von TV-Moderator Ralph Caspers als gut gelauntes Tandem durch den Abend. Vor allem, dass so viele junge Leute sich an dem Wettbewerb beteiligten, habe die Jury begeistert, sagte Spaeing.

Barbara Thiel, Landesbeauftragte für den Datenschutz in Niedersachsen, stimmte dem zu. „Wir nehmen häufig wahr, dass sich die Öffentlichkeit nicht so sehr für Datenschutz interessiert. Auch die Politik nicht wirklich. Umso wunderbarer ist es, dass sich junge Menschen damit so intensiv beschäftigen."

Aber Thomas Spaeing denkt dabei auch an die Zukunft: „Kinder und Jugendliche, die heute selbstverständlich im Netz surfen, sind diejenigen, die später in der Wirtschaft verantwortungsvolle Aufgaben übernehmen. Wenn wir sie jetzt mit dem Thema Datenschutz erreichen, dann werden sie in ihrem Berufsleben viel bewusster an das Thema herangehen", sagte er.

Die gute Resonanz auf die zweite DAME-Ausschreibung, an der sich mit 39 Einreichungen fast 60 Prozent mehr als bei der ersten Preisverleihung beteiligten, will der BvD nutzen, um die DAME und die BvD-Initiative „Datenschutz geht zur Schule" in einen eigenen, gemeinnützigen Verein miteinander zu verbinden.

Alle Informationen, Videos, und Bilder zum Datenschtutz Medienpreis (DAME) finden Sie unter: *www.bvdnet.de/datenschutzmedienpreis/*

BvD-News: Bei der zweiten DAME-Runde haben sich sehr viel mehr Medienschaffende beworben. Wie geht es weiter mit der DAME?

Thomas Spaeing: Viele Wettbewerbsbeiträge zielen auf Kinder und Jugendliche, sie treffen deren Sprache und die Themen, die die jungen Zielgruppen im Alltag mit Smartphones und Tablets haben. Damit ergänzen die Beiträge wunderbar unsere Initiative „Datenschutz geht zur Schule." Deshalb wollen wir beide Projekte mittelfristig in einem gemeinnützigen Verein zusammenführen.

BvD-News: Was ist der Vorteil einer solchen Übertragung?

Thomas Spaeing: Ein gemeinnütziger Verein kann Spenden einwerben und annehmen. Das kann der BvD leider nicht. Aber bereits in der Vergangenheit haben wir bei „Datenschutz geht zur Schule" und seit November 2018 auch bei der DAME von der Unterstützung der DATEV-Stiftung Zukunft profitiert. In einem gemeinnützigen Verein ist das wesentlich einfacher zu verwalten.

HANDBUCH EUROPÄISCHES UND DEUTSCHES DATENSCHUTZRECHT

Prof. Dr. Louisa Specht und Dr. Reto Mantz (Hrsg.)

Prof. Dr. Louisa Specht und Dr. Reto Mantz (Hrsg.)
»Handbuch Europäisches und deutsches Datenschutzrecht«

C.H. Beck Verlag

1. Auflage 2019, 788 Seiten/ 372 Seiten – broschiert
ISBN 978 3 406 72539 5
109,00 Euro

Das neue Handbuch soll eine praxisbezogene und zugleich wissenschaftlich fundierte Darstellung zum europäischen und deutschen Datenschutzrecht sowie der Schwerpunkt die Lösung konkreter Anwendungsfragen der Datenschutz-Grundverordnung und des neuen Bundesdatenschutzgesetzes und der zahlreichen neuen bereichsspezifischen Datenschutzregelungen in Bund und Ländern, die seit 2018 gelten, sein. Dies gelingt den Herausgebern mit dem Handbuch und den von ihnen hierfür gewonnenen Autoren eindeutig!

Anders als die zum Thema erschienen Kommentare und Datenschutzbücher wird in diesem Handbuch das Datenschutzrecht nicht anhand seiner Einzelregelungen oder durch die DSGVO vorgegebenen Themenzusammenhänge, sondern anhand von Sektoren bzw. Branchen behandelt. Dies bietet natürlich den Vorteil, das Spezielle aber vor allem auch das Allgemeine bereits auf dieses Thema bezogen darzustellen. Das Handbuch eignet sich also hervorragend für eine „branchenproblemorientierte" Einarbeitung aber ebenso als „branchenproblemorientiertes" Nachschlagewerk. Gleichwohl verzichtet es (zu Recht) nicht auf die Darstellung der datenschutzrechtlichen Grundlagen in seinem Teil A. In Teil B schließen 11 Datenschutzthemen der Privatwirtschaft (Verbraucherdatenschutz,Beschäftigtendatenschutz, Datenschutz in der Anwaltschaft, Datenschutz in der Privatversicherung, Datenschutz im Medizinsektor, Datenschutz im Finanzwesen, Datenschutz in der Informationstechnik, Datenschutz im Automotive-Sektor, Datenschutz im Energiesektor, Datenschutz im Telekommunikationssektor, Datenschutz in Presse und anderen Medien) und sodann in seinem Teil C weitere 8 Datenschutzthemen im öffentlichen Sektor (Datenschutz in der Verwaltung von Bund, Ländern und Kommunen, Datenschutz und präventive Tätigkeit der Polizei, Datenschutz in der Justiz, Datenschutz in Forschung und Hochschullehre, Datenschutz in Schule und Schulverwaltung, Datenschutz in Kultureinrichtungen, Bibliotheken und Archiven, Sozialdatenschutz, Kirchliches Datenschutzrecht) an. Den Herausgebern ist dabei eine gute und zugleich praxisorientierte Zusammenstellung der behandelten Themen gelungen.

Das Handbuch ist übersichtlich gestaltet und diskutiert die Rechtsfragen verständlich, praxisgerecht und „branchenproblemorientiert"

Rezensionen von

Dr. Jens Eckhardt
Rechtsanwalt
Fachanwalt für Informationstechnologierecht
Datenschutz-Auditor (TÜV)
Compliance Officer (TÜV)
Vorstandsmitglied des BvD e.V.

IT-OUTSOURCING UND CLOUD-COMPUTING

Peter Bräutigam (Hrsg.)

PETER BRÄUTIGAM (HRSG.)
»IT-Outsourcing und Cloud-Computing«

ERICH SCHMIDT VERLAG

4. völlig neu und bearbeitete und Auflage 2019
1.480 Seiten
ISBN-13: 978-3503181735
176,00 Euro

Die Autoren sind alle in der beratenden Praxis bzw. in der wissenschaftlichen Lehre tätig. Das Werk befasst sich nur in Teilaspekten mit Datenschutz – gerade das macht den umfassenden und hervorzuhebenden Anspruch dieses Werkes aus.

In insgesamt 16 Teilen werden die unterschiedlichen Thematiken des IT-Outsourcings dargestellt. Zum Thema Datenschutz befassen sich explizit der gesamte 5. Teil und der Unterteil B des 14. Teils (Cloud-Computing) damit. Auch wenn sich damit „nur" ca. 10 % des Werkes mit dem Thema Datenschutz befassen, ist es insbesondere aus Datenschutzsicht empfehlenswert! Jedem Praktiker ist es ein Graus, wenn in komplexen Projekten immer nur Teilaspekte bewertet werden und nie alle relevanten Aspekte gemeinsam einer zusammenfassenden Bewertung zugeführt werden. Durch die in dem Buch umfassend dargestellten Inhalte wird dies ermöglicht. So gibt Teil 1 eine Einführung in die technischen und wirtschaftlichen Grundlagen von IT-Outsourcing-Projekten, bevor im 2. Teil auch unter grafischen Darstellungen die rechtlichen Ausgangspunkte erläutert werden.

Mit der zivilrechtlichen Einordnung von IT-Leistungen befasst sich der 3. Teil.

Die im 4. Teil dargestellten Anforderungen aus urheberrechtlicher Sicht werden in der Praxis bei etlichen Auslagerungen unterschätzt. Hier werden u.a. Fragestellungen, ob eine proprietär erworbene Software / Datenbank auch durch einen anderen betrieben werden darf, erläutert und Hinweise zur Beantwortung gegeben.

Arbeitsrechtliche Grundlagen in Teil 6, gesellschafts- und konzernrechtliche Grundlagen in Teil 7 sowie die steuerrechtlichen Besonderheiten in Teil 8 runden die allgemeinen Themen ab, bevor branchenspezifische Anforderungen in Teil 9 (Kredit- und Finanzdienstleistungen), in Teil 10 (Öffentliche Hand) und Teil 11 (Sozial- und Gesundheitswesen) behandelt werden. Darstellungen zur rechtliche Vorbereitungen und Vertragsverhandlung (Teil 12) und zur Vertragsgestaltung (Teil 13) unterstützen den allumfassenden Anspruch des Werkes. Die Ausführungen zum Cloud-Computing im speziellen (Teil 14) sind strukturiert aufgebaut und umfassen alle relevanten Probleme auch im Drittstaatenverkehr. Mit Ausführungen zu strafrechtlichen Aspekten (Teil 15) und einem Glossar (Teil 16) schließt das Werk.

Besonders erfreut hat mich an dem Werk die Berücksichtigung bestimmter Branchenstandards wie den bankaufsichtlichen Anforderungen an die IT (BAIT) oder auch die Darstellung der Anforderungen der Auslagerung von Informationen, die dem Schutzbereich des § 203 StGB unterliegen.

Während man die dargestellten Grundthematiken des Datenschutzrechts bei Datenschutzbeauftragten erwarten kann, wenn nicht gar muss, ist es auch hinsichtlich der Detailtiefe für alle empfehlenswert.

Das Werk eignet sich darüber hinaus insbesondere für Praktiker*innen in Unternehmen und Kanzleien, von denen eine rechtliche Gesamtbetrachtung erwartet wird und nicht nur die Beantwortung einer Einzelfrage aus dem Datenschutzrecht.

BETRIEBLICHER DATENSCHUTZ

Forgó / Helfrich / Schneider (Hrsg.)

FORGÓ / HELFRICH / SCHNEIDER (HRSG.)
»Betrieblicher Datenschutz«

C.H. BECK VERLAG

3. Auflage 2019
1.639 Seiten
ISBN-13: 978-340672579
249,00 Euro

Das Autorenteam dieses Rechtshandbuchs umfasst neben den Herausgebern renommierte Datenschutzexperten und Praktiker. Sie eint das Ziel, mit diesem Werk einen Beitrag zur Interpretation des Datenschutzrechts auf Basis der DSGVO, aber auch unter Berücksichtigung des nationalen Rechts und angrenzender Rechtsgebiete zu leisten. Positiv hervorzuheben ist, dass sich dieses Werk nun in der 3. Auflage auch der Interpretation und Umsetzung des Datenschutzrechts in anderen Mitgliedsstaaten befasst. So erhält jeder Teil einen Annex zur Darstellung der Thematik in Österreich und in einem eigenen Teil wird die Umsetzung in insgesamt 7 weiteren europäischen Staaten ausgeführt, wobei sich die Auswahl nicht auf Mitgliedsstaaten der EU begrenzt.

Das Rechtshandbuch gliedert sich in 15 Teile, beginnend mit den allgemeinen Grundlagen, gefolgt von der Datenschutzorganisation, den Informationspflichten, der Thematik der Archivierung und Entsorgung und der Darstellung Datenschutz und Personal. Ausführungen zu Datenschutz in Betrieb, Unternehmen und Konzern werden ergänzt um Outsourcing und neue Technologien sowie in verschiedene Kommunikationsformen. Eigene Teile gibt es auch zu eCommerce und Datenschutz im Gesundheitssektor. Die Anforderungen an die Datensicherheit und das Konfliktmanagement schließen die Darstellungen ab, bevor im letzten Teil die rechtlichen Umsetzungen in Großbritannien, Italien, Schweden, Tschechien, Schweiz, Russland und der Ukraine skizziert werden.

Innerhalb der Teile erfolgt die Aufteilung in Kapitel und ermöglicht eine sehr detaillierte Darstellung der einzelnen Themengebiete. Die Gestaltung der Teile bringt es mit sich, dass beispielsweise eine zentrale Thematik wie die Auftragsverarbeitung an mehreren Stellen unter den jeweiligen Aspekten behandelt wird und nicht in einer linearen Themendarstellung. Für den Praktiker mit Vorerfahrung ist dies bei der Lösung von einzelnen, konkreten Fragestellungen sehr hilfreich, wird sich jedoch weniger für Einsteiger eignen, die sich den ersten Überblick verschaffen möchten. Besonders erfreulich ist, dass sich die jeweilige Darstellung nicht nur auf der Wiedergabe einer gfls. herrschenden Meinung beschränkt, sondern auch Kritikpunkte und Diskussionsbeiträge liefert. Dies ermöglicht bei komplexen Fragenstellung die Erarbeitung einer eigenen Positionierung im Beratungsfall.

Das Rechtshandbuch ist uneingeschränkt empfehlenswert für die Leser, die sich mit komplexen Fragestellungen befassen und Lösungen suchen, die sich auch begründen lassen.

Rezensionen von

Rudi Kramer
Rechtsanwalt (Syndikusrechtsanwalt),
DATEV eG, und Sprecher AK Schule des BvD e. V.

DATENSCHUTZ IM GESUNDHEITSWESEN

Benedikt Buchner (Hrsg.)

Benedikt Buchner (Hrsg.)
»Datenschutz im Gesundheitswesen«

AOK Verlag, Remagen

2. Aufl. 2019
ISBN 978-3-553-43110-1
89,90 Euro

„Die Broschüre soll Datenschutzverantwortlichen dabei helfen, die Datenverarbeitung in Gesundheitseinrichtungen auch künftig rechtskonform zu gestalten. Das Handbuch vermittelt die neuen gesetzlichen Grundlagen, führt praxisnah in die Datenschutzorganisation ein und erläutert am Beispiel des Krankenhauses die zentralen datenschutzrechtlichen Herausforderungen." Dies ist laut Klappentext die Zielsetzung des Buches.

Das 380-seitige Handbuch ist in fünf Teile untergliedert: rechtliche Grundlagen (79 S.), Datenschutzorganisation (94 S.), Datenschutz im Krankenhaus (59 S., Internetauftritt (44 S.), IT-Sicherheit (69 S.)

Die rechtlichen Grundlagen verweisen zwar darauf, dass es spezialgesetzliche Regelungen wie Landeskrankenhausgesetze, Sozialgesetzbücher oder Berufsordnungen gibt, deren Inhalt bleibt den Lesenden jedoch verschlossen. Das Handbuch bietet Neu-Einsteigern im Datenschutzrecht eine fundierte Einführung in die Grundlagen des Datenschutzrechts wie beispielsweise Einwilligung oder Betroffenenrechte, aber auf 79 Seiten können die rechtlichen Grundlagen im Gesundheitsdatenschutz nicht dargeboten werden. Um beispielsweise zu erfahren, wie eine Auftragsverarbeitung und insbesondere ein entsprechender Vertrag zu gestalten ist, wird weitergehende Literatur (oder andere Informationsquellen) benötigt. Hier enthält das Buch aber in den jeweiligen Abschnitten Hinweise, wo weitergehende Informationen zu finden sind.

Das Thema Datenschutzorganisation ist das umfassendste Kapitel des Handbuchs. Darin wird u. a. auf die Benennungspflicht des Datenschutzbeauftragten eingegangen, aber auch auf Themen wie die Bestandsaufnahme oder Audits – alles wird in Anbetracht der geringen Seitenzahl thematisch nur angerissen, aber so wird den Lesenden vermittelt, an was er alles zu denken hat.

Im dritten Kapitel „Datenschutz im Krankenhaus" wird auf mehreren Seiten auf den Internetauftritt eingegangen; in Anbetracht, dass sich das vierte Kapitel diesem Thema widmet, hätte man diese Seiten besser zur Einführung in die Besonderheiten des Gesundheitsdatenschutzes genutzt. Denn obwohl in diesem Kapitel auf krankenhausspezifische Themen wie Patientenaufnahme und Behandlungsvertrag eingegangen wird, fehlen wichtige Hinweise. So wird beispielsweise eine Einwilligung bzgl. Weitergabe von Daten an Hausarzt/Facharzt angesprochen, aber leider nicht erwähnt, dass die Definition des Begriffs „Hausarzt" sich in § 73 Abs. 1a SGB V findet. Das Kapitel enthält für alle Personen, die sich im Krankenhauswesen nicht auskennen, eine gute Einführung in den organisatorischen Ablauf der Patientenversorgung, wobei die rechtlichen Rahmenbedingungen leider nicht erläutert werden.

Da heutzutage jedes Krankenhaus und nahezu jede Arztpraxis über einen Internetauftritt verfügen ist es sicherlich richtig, dass die Autoren dieses Thema aufgriffen. Die 44 Seiten enthalten eine gute Einführung ins Thema, allerdings sollten hier Hinweise auf weitergehende Informationsquellen erfolgen. Die im Handbuch enthaltenen Informationen bzgl. Impressum oder Umgang mit Social Media Plug-ins alleine reichen sicherlich nicht aus, dass die Lesenden anschließend das Thema bearbeiten können.

Im letzten Kapitel werden aktuelle Gesetzgebungsverfahren zur IT-Sicherheit vorgestellt. Gerade da diese Gesetze in der Öffentlichkeit oftmals nicht so stark diskutiert werden, stellt dies eine hilfreiche Information für den Datenschutzbeauftragten dar.

Kleine Inkonsistenzen sind natürlich vorhanden. So wird in einem „Tipp" bzgl. Datenschutz-Folgenabschätzung dazu geraten, auf die Black- und White-Listen der Aufsichtsbehörden zurückzugreifen, aber gerade die White-Liste existiert in Deutschland nicht; dieses Wissen würde man bei den Autoren eigentlich voraussetzen. Insgesamt stellt das Handbuch eine empfehlenswerte Lektüre für jeden dar, der sich in die Datenschutz-Thematik und insbesondere in die DSGVO einarbeitet. Da die Autoren auf den wenigen Seiten nicht auf die verstreute nationale Bundes- und Landes-Gesetzgebung zum Gesundheitsdatenschutz (wie z. B. Arzneimittelgesetz, Sozialgesetzbücher, Medizinprodukterecht bzw. Rettungsdienstgesetze, Krankenhausgesetze) eingingen, enthält das Handbuch für erfahrenere Datenschützer wenig Neues.

Rezension von

Dr. Bernd Schütze
Deutsche Telekom Healthcare and Security Solutions GmbH
Experte für: Medizinische Informatik, Datenschutz, Datensicherheit,
Mitglied im BvD e.V.

DATENSCHUTZRECHT FÜR SCHWEIZER UNTERNEHMEN – DSGVO

Benjamin Domenig, Christian Mitscherlich

Benjamin Domenig, Christian Mitscherlich
»Datenschutz für Schweizer Unternehmen«

Stämpfli verlag, bern

2. Aufl. 2019
ISBN 978-3-553-43110-1
78,00 CHF (ca. 72,00 Euro)

Das Buch richtet sich explizit an schweizerische Unternehmen – an Unternehmer, Verwaltungsräte, Geschäftsleitungsmitglieder und Stabstellen. Es gibt einen Überblick über das breite Spektrum der neuen Regeln der Datenschutzgrundverordnung (DSGVO) aus Schweizer Sicht.

Es erläutert leicht und verständlich anhand von Fallbeispielen die Anwendbarkeit der DSGVO. Mehrere Beispiele aus Unternehmen begleiten den Leser durch das Buch. Mit Hilfe von Fallbeispielen werden Szenarien skizziert und mögliche Lösungsansätze für den Tatbestand gegeben.

Ein besonderes Augenmerk wird auf die Bereiche Erlaubnistatbestände, Auftragsverarbeitung, Informationsrechte sowie Rechte der betroffenen Personen gerichtet. Dabei werden im Gesetz verwendete Begrifflichkeiten erläutert. Url-Angaben verweisen auf weitere Informationen. So werden z.B. die Erlaubnistatbestände ausführlich und anhand von Beispielen erklärt. Mit Hilfe von Abbildungen werden Sachverhalte anschaulich dargestellt.

Im Kapitel „Anforderungen an die Unternehmensstruktur" finden sich Handlungsempfehlungen, um den Nachweispflichten nachzukommen sowie allgemeine Hinweise für z. B. IT-Sicherheit. Außerdem werden die Aufgaben des Datenschutzbeauftragten – bzw. für den Ansprechpartner für Datenschutz – beschrieben und die Verantwortung für das Unternehmen dargelegt.

Immer wieder findet sich der Hinweis, sich im Bedarfs- und Zweifelsfalle an einen Datenschutzexperten zu wenden. Dies gilt allerdings nicht nur für Schweizer Unternehmen.

Das Buch ist empfehlenswert für jeden, der sich einen allgemeinen Überblick über die DSGVO verschaffen möchte und ist besonders für kleine und mittelgroße Unternehmen geeignet.

DIE OPTIMIERER

Theresa Hannig

Theresa Hannig
»Die Optimierer«
Roman

Bastei Lübbe AG, Köln

2017, 304 Seiten
ISBN 978-3-404-20887-6
Taschenbuch 10,00 Euro/Kindle 8,99 Euro

Referenten und Moderatoren erhalten vom BvD ein kleines Dankeschön. Bei den BvD-Verbandstagen 2019 wurde diesmal der Roman „Die Optimierer" überreicht.

Dieser wurde mit dem Stefan-Lübbe-Preise 2016 und dem Seraph 2018 für das beste Debüt ausgezeichnet.

„Die Optimierer" ist ein dystopischer Roman und spielt in München des Jahres 2052 (das Oktoberfest gibt es noch). Hauptfigur ist Samson Freitag, ein junger und nicht gerade „netter Mann von nebenan". Er arbeitet als Lebensberater bei der sympathisch klingenden „Agentur für Lebensberatung" im Überwachungsstaat BEU (Bundesrepublik Europa).

In der Welt von „Die Optimierer" geht es den Menschen gut. Sie leben in einer Optimalwohl-Ökonomie. Jeder hat den passenden Job und wenn jemand nicht arbeiten will oder einfach ungeeignet ist, ist das für die Gesellschaft kein Problem – „Jeder an seinen Platz!", so das Motto und die Begrüßung in der BEU. Es gibt autonomes Fahren, riesige Clouds für die Daten und „Sozialpunkte", nach denen Menschen bewertet werden. Smarte Roboter sorgen für die Sicherheit und erledigen die meiste Arbeit.

Kurz vor seiner Beförderung (es fehlen Samson nur noch wenige Sozialpunkte), begeht eine Bürgerin nach einer Lebensberatung Selbstmord. Sein regelmäßiges, bequemes und konformes Leben gerät aus den Fugen. Er „verliert" seine Eltern, seine Freundin, seine Kollegen … und seine Sozialpunkte. Samson gerät in die Mühlen des überwachenden Optimierungssystems. Es beginnt ein Kampf um Anerkennung und Rückkehr in das konforme Leben. Am Ende muss Samson feststellen, dass … aber lesen Sie selbst.

Die Autorin, Theresa Hannig, geb. 1984 in München, studierte Politikwissenschaft an der Uni München. In einem Interview (Süddeutsche Zeitung vom 28.09.2017; Florian J. Haamann „Eine düstere Zukunft" https://www.sueddeutsche.de/muenchen/fuerstenfeldbruck/szenische-lesung-eine-duestere-zukunft-1.3685658) sagte sie, dass sie den Roman politisch verstanden wissen und zeigen wolle, „wohin es führen kann, wenn immer mehr Daten gesammelt werden, nämlich zu einem Verlust von Freiheit, wenn etwa eine extremistische Partei an die Macht komme."

Das Buch steht in bester Tradition mit den großen Dystopien der Literaturgeschichte, Aldous Huxleys „Schöne neue Welt" und George Owells „1984". Es beschreibt eine Zukunft, welche in Teilen schon Gegenwart, in Teilen schon ganz nahe ist.

Fazit: Absolut lesenswert!

Rezensionen von
Regina Mühlich
Geschäftsführerin der AdOrga Solutions GmbH
Datenschutzbeauftragte, Datenschutz-Auditorin,
Compliance Officer, Vorstandsmitglied des BvD e. V.

Anzeige

29

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.

PRIVACYSOFT ist eine Marke von Projekt 29 GmbH & Co. KG

KOMPLETTE Datenschutzdokumentation
EXTRA Vorlagen und Checklisten
NEUES Auditmodul
BEWÄHRTE Online-Schulungen
DE/EN/FR Mehrsprachig

DAS DSB-MULTI-TOOL FÜR DEN DATENSCHUTZ NACH EU-DSGVO

INNOVATIONSPREIS-IT BEST OF 2018 initiative mittelstand IT-SECURITY
Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft
Software Hosted in Germany Bundesverband IT-Mittelstand e.V.
bevh PREFERRED BUSINESS PARTNER
BvD e.V. MITGLIED DATENSCHUTZ GESTALTEN

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

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

Die wichtigsten Daten der BvD-Gremien

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

▶ www.bvdnet.de/regionalgruppen **bzw.**

▶ www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

17.09.2019	RG Ost	**18.10.2019**	RG Karlsruhe
26.09.2019	RG Gütersloh	**28./29.10.2019**	AK Medizin
27./28.09.2019	AK Externe	**28.11.2019**	RG Gütersloh
11.10.2019	RG Stuttgart	**28.11.2019**	RG Ost
17.10.2019	AK Finanzdienstleistung	**17.01.2020**	AK Entsorgungs- und Versorgungsunternehmen (AK EVU)
17.10.2019	AK Sozial		
17.10.2019	RG Mitte		
18.10.2019	AK Krypto	**22.01.2020**	AK Sozial
18.10.2019	RG München	**31.01./01.02.2020**	AK Externe
18.10.2019	RG Nürnberg		

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

Termine und Anmeldung finden Sie auf unserer Webseite:

▶ www.bvdnet.de

VERNETZEN SIE SICH MIT UNS:

▶ www.bvdnet.de

XING: https://www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

TWITTER: www.twitter.com/bvd_datenschutz

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

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

BVD-STELLENBÖRSE

Sie suchen ausgewiesenes Datenschutz-Knowhow für Ihr Unternehmen? Mit einer Anzeige in der BvD-Stellenbörse finden

Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:

▶ https://www.bvdnet.de/bvd-stellenboerse/

Anzeige

WEPRIDO
DATA PRIVACY MANAGEMENT

DATENSCHUTZ? – SCHON ERLEDIGT.

WEPRIDO – Die Datenschutz-Management-Software, die Datenschutz einfach macht.

- **Multi-User-fähig** bis zu fünf Benutzer pro Unternehmen
- **Smarte Benutzerführung** bei Datenschutz Selbstadministration
- **Digitale DSGVO**-Compliance Lösung
- **Verzeichnis** für Verarbeitungstätigkeiten mit zahlreichen Vorlagen
- **Online Datenschutzhandbuch** mit methodischer Struktur
- **Umfangreiche Checklisten** für TOMs und Webchecks
- **Ticket- und Erinnerungssystem** für simples Aufgabenmanagement
- **Automatisierte E-Mail-Benachrichtigungen**

Für Ein-Mann-Unternehmen, Mittelstand oder Konzern, **WEPRIDO** passt sich Ihren Datenschutzbedürfnissen an.

WEPRIDO IST FÜR EXTERNE DATENSCHUTZ-BEAUFTRAGTE KOSTENLOS!*

*) Das Lizenzmodell von **WEPRIDO** basiert auf dem Grundsatz, dass die Benutzung für einen externen Datenschutzbeauftragten **kostenfrei** bleibt und nur die betreuten Unternehmen benötigen einen kostenpflichtigen Account. Lizenzgebühren bezahlt also nicht der Datenschutzbeauftragte, sondern stets das oder die zugeordneten Unternehmen. Preise für kostenpflichtige Tarife finden Sie unter www.weprido.eu. Monatliche Gebühren ab 49,99 € (zzgl. der ges. MwSt.). Monatlich kündbar.

creativparc.com foto: yakobchuk olena / adobestock.com

Sie haben noch Fragen? – Wir sind für Sie da.

Nehmen Sie direkt mit uns Kontakt auf.
Unsere Experten stehen Ihnen jederzeit per Mail unter support@weprido.eu oder per Telefon unter +49 (0) 800 800 80 60 zur Verfügung.

Montag – Donnerstag von 9 – 17 Uhr; Freitag von 9 – 12 Uhr.

www.weprido.eu

WEPRIDO ist eine Marke der aiho Service GmbH
Goldener Steig 42, 94116 Hutthurm

Anzeige

LEITZ IQ-SHREDDER
DER PAPIERKORB 2.0 – GEH AUF NUMMER SICHER

Tina I. aus Leipzig
Human Ressources

€ 20.0 MIO SPAREN!*

*Schreddern unterstützt die Einhaltung der DSGVO. Verstöße gegen die DSGVO können mit Bußgeldern von bis zu € 20.0 Mio oder 4 % des weltweiten Jahresumsatzes des entsprechenden Unternehmens geahndet werden – je nachdem, welche Summe größer ist.

DSGVO KONFORM

Wenn es um Datenschutz geht, ist es wichtig, keine unnötigen Risiken einzugehen. Mit einem Leitz IQ-Shredder unter Ihrem Schreibtisch sind Sie auf der sicheren Seite – denn dieser ist die intelligente Alternative zu einem Papierkorb. Er ist der Papierkorb 2.0.

Mehr unter:
www.leitz.com/shredder

LEITZ®
ALLES IM GRIFF