Ausgabe 02/2020

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Digitale Ethik

Datenschutz und Verantwortung

ZWEI JAHRE DSGVO - DIE BILANZ DER EU-KOMMISSION – S. 46

KEINE AUFTRAGSVERARBEITUNG DURCH STEUERBERATER – S. 62

DATENVERARBEITUNG VON DER BEWERBUNG BIS ZUM JOBWECHSEL – S. 66

UNBOXING STATT GLITTERKANONE - DIE DAME 2019 FAND ONLINE STATT – S. 76

BvD e.V.

DATENSCHUTZ GESTALTEN

Jetzt anmelden:
https://www.bvdnet.de/termine/verbandsveranstaltung/

2020

BvD-Herbstkonferenz & Behördentag

14.10. - 16.10.2020

Hybrid-Veranstaltung, Teilnahme auch online möglich

>> Datensammeln – mobil – international – legal(?) <<

mit folgenden Themen:

- Datenschutz und Cloud
- Schadenersatzansprüche nach DSGVO
- Cybersicherheit
- Highlights im Datenschutzjahr
- u. v. m.

in Kooperation mit:

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

BayLDA

BvD e.V. DATENSCHUTZ GESTALTEN

EDITORIAL

Liebe Leserinnen und Leser,

der Megatrend Digitalisierung beschäftigt uns als Datenschützer nicht erst seit dem Ausbruch der Corona-Pandemie. Bereits letztes Jahr im Sommer war beispielsweise Künstliche Intelligenz das Titelthema unserer BvD-News und des BvD-Kongresses in Berlin. Mit Corona allerdings hat diese Entwicklung noch einmal einen massiven Schub bekommen. So verwundert es nicht, dass in den Diskussionen um die immensen Förderpakete, die derzeit geschnürt werden, Rufe laut werden, in diesem Zusammenhang auch in eine digitale deutsche und europäische Infrastruktur zu investieren und die Wirtschaft bei der Umstellung von Unternehmensprozessen zu unterstützen. Eine berechtigte Forderung, die auch der BvD aktiv unterstützt. Doch sollte dies nicht in eine reine Technikdebatte führen. Denn woran es oftmals besonders im Mittelstand mangelt, ist das Know-how in der Implementierung digitaler Prozesse und komplexer IT-Lösungen – Stichwort: Fachkräftemangel. Hier können unter anderem Datenschutzbeauftragte wertvolle anbieterunabhängige Beratung in Unternehmen einbringen und dies machen sie bereits seit Jahren. Die Politik täte gut daran, auch in diesem Bereich Anreize zu schaffen – also auch diese Beratung zu fördern.

Neben technischen, rechtlichen und wirtschaftlichen Aspekten, spielen bei der Digitalisierung mehr und mehr auch ethische Fragestellungen eine Rolle. Auf staatlicher und unternehmerischer Ebene stehen Datenethik und speziell digitale Ethik bereits länger auf der Agenda. Mehr und mehr erhält die Thematik aber auch in der Zivilgesellschaft Aufmerksamkeit, man denke nur an die lebhaften Debatten über die Corona-Warn-App. Die verschiedenen Ebenen spiegeln sich auch in den Artikeln zu unserem Schwerpunktthema wider: Umfassende Einblicke über die unterschiedlichen Problemstellungen bieten die Artikel von Petra Grimm, Bernd Schütze und Nikolai Horn, wobei Letzterer auch die Rolle des Datenschutzbeauftragten im organisationsübergreifenden Reflexionsprozess beleuchtet, als welchen Horn digitale Ethik begreift. Marit Hansen gibt Einblicke in ihre Arbeit als Mitglied der Datenethikkommission der Bundesregierung und Angelika Pauwer und Christiane Wendehorst greifen in ihren Artikeln zu „Corporate Digital Responsibility“ und Algorithmen-Haftung unternehmerische Praxisaspekte des Themas auf. Andrea Jelinek, die Vorsitzende des Europäischen Datenschutzausschusses, schließlich zeigt auf, inwiefern datenethische Überlegungen in der DSGVO in eine rechtliche Form „gegossen“ wurden und sich in juristische Konkretisierung auch in den Dokumenten des EDSA niederschlagen, die den nationalen Aufsichtsbehörden als Auslegungshilfen dienen sollen.

Apropos Aufsichtsbehörden – Vor dem Hintergrund des in der Datenethik zentralen Werts der informationellen Selbstbestimmung kommt den Aufsichtsbehörden laut Nikolai Horn auch die Verantwortung als „Vertrauensanker“ zu: Sie stehen dem Individuum bei der Überwindung der Machtasymmetrie beim Durchsetzen seines Rechts auf informationelle Selbstbestimmung gegenüber Unternehmen zur Seite. Wie umfassend sie diese wichtige Funktion noch erfüllen könnten, falls die derzeit wiederauflebende Bestrebung Erfolg haben sollte, die Unternehmensaufsicht in einer zentralen Bundesbehörde zu bündeln, ist fraglich. Welche weiteren Argumente für und gegen eine Zentralisierung ins Feld geführt werden könnten, wird der BvD im Herbst gemeinsam mit der Stiftung Datenschutz in einem Expertenpanel unter dem Titel „Zukunft der Datenschutzaufsicht“ ergebnisoffen diskutieren. Wir werden Sie dazu auf dem Laufenden halten.

Die Herbsttagung naht in großen Schritten und uns haben viele Anfragen erreicht, ob denn ein „echtes Treffen“ wieder möglich sei. Nachdem das Hotel in Stuttgart uns dafür eine Absage erteilt hat, haben wir geeignete Räume in Mannheim gefunden und werden dort, so es die Situation dann erlaubt, eine Hybrid-Veranstaltung durchführen. Wer kann und möchte, kommt nach Mannheim in den Rosengarten und wer vom Büro aus teilnehmen möchte, der bucht sich online ein. Das ist für den BvD ein Novum und eine echte Herausforderung. Die Mitgliederversammlung wird dann allerdings nicht digital stattfinden, sondern in Mannheim vor Ort abgehalten. Der Termin wurde aus diesem Grund eine Woche vorverlegt. Bitte achten Sie auf die Ankündigungen dazu.

Ich wünsche Ihnen eine anregende Lektüre.

T. Spaeing

Ihr Thomas Spaeing
BvD-Vorstandsvorsitzender

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

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

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

Fotos:
123rf.com

Lektorat:
Frank Spaeing, Regina Mühlich

Anzeigen:
Christina Denz
Kooperationen: Karsten Füllhaase
(bvd-gs@bvdnet.de)

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

ISSN: 2194-1025
Erscheinungsweise: 3 x jährlich, ca. 4.000 Exemplare
(Unsere Mediadaten erhalten Sie unter bvdnet.de/Publikationen oder in der Geschäftsstelle (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

Thomas Spaeing 3

DIGITALE ETHIK

Datenethische Aspekte im Zusammenhang mit der Arbeit des Europäischen Datenschutzausschusses – *Dr. Andrea Jelinek und Barbara Chlopcik* 5
Digitale Ethik als Reflexionsprozess – *Dr. Nikolai Horn* 9
Datenschutz und Ethik: Widerspruch oder Harmonie? – *Bernd Schütze* 17
Digitale Ethik und Ethics by Design – *Prof. Dr. Petra Grimm* 24
Mehr (als) Datenschutz: Plädoyer für ein planvolles Vorgehen für Datenschutz by Design – *Marit Hansen und Benjamin Bremert* 30
Kontrolle und Haftung bei Algorithmischen Systemen – *Prof. Dr. Christiane Wendehorst* 35
Corporate Digital Responsibility – ein digitalethischer Kompass – *Angelika Pauer, Saskia Becke, Daniela Hanauer und Paul Czech* 40

DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)

Der Bericht der EU-Kommission zur Evaluierung der DSGVO zwei Jahre nach ihrem Start – *Dr. Tilman Dralle* 46
Sicherheit der Verarbeitung – *Dr. Gunther Schlöffel* 50

GESETZESÄNDERUNGEN UND RECHTSPRECHUNGEN

Zuverlässigkeit und Qualifikation des Datenschutzbeauftragten – *Dr. Carlo Piltz und Philipp Quiel* 56

DATENSCHUTZPRAXIS

Keine Auftragsverarbeitung durch Steuerberater – *Rudi Kramer und Nicole Schmidt* 62
Datenverarbeitung von der Bewerbung bis zum Jobwechsel – *Caroline Gigger und Jutta Sonja Oberlin* 66

AUFSICHTSBEHÖRDEN

„Corona kam für uns etwas zu früh." – *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Stefan Brink, im Interview mit den BvD-News* 72

AUS DEM VERBAND

Full House online - Rund 800 Teilnehmer bei der ersten virtuellen Video-Ausgabe der BvD-Verbandstage – *Karsten Füllhaase* 74
Neue Erfahrungen nicht nur für Dozenten – *Regina Mühlich* 75
Unboxing statt Glitterkanone - Die DAME-Preisverleihung fand in diesem Jahr online statt – *Christina Denz* 76

REZENSIONEN

Datenschutz & Marketing – *Dr. Jens Eckhardt* 80
Rechtshandbuch Cyber-Security – *Tobias Heinrich, Alexander Kiefner, Detlev Gabel (Hrsg.)* 82
Informationssicherheit und Datenschutz – *Secorvo Security Consulting (Hrsg.)* 84
Rechtshandbuch Industrie 4.0 und Internet of Things – *Thomas Sassenberg, Tobias Faber (Hrsg.)* 86

TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 87

DATENETHISCHE ASPEKTE IM ZUSAMMENHANG MIT DER ARBEIT DES EUROPÄISCHEN DATENSCHUTZAUSSCHUSSES

Dr. Andrea Jelinek und Mag. Barbara Chlopcik

In den Medien gibt es oft einen kritischen Aufschrei zum Thema Datenschutz.

Neben wirtschaftlichen Interessen liegt der Fokus – nicht zuletzt bedingt durch die COVID-19-Pandemie und die damit einhergehenden Bestrebungen zur Bekämpfung des Virus – insbesondere auf ethischen Fragestellungen im Bereich des Datenschutzes, der sogenannten Datenethik. Verkannt wird hierbei oft, dass Datenethik und insbesondere digitale Ethik im Allgemeinen keine neuen Bereiche unseres Lebens sind. Themen, die heute hitzige Diskussionen in der breiten Öffentlichkeit entfachen, wurden während der letzten Jahrzehnte in Expertenkreisen diskutiert und werden, nicht zuletzt wegen der rasanten technologischen Entwicklungen, auch in Zukunft von Relevanz sein. Die Suche nach Antworten auf ethische Fragestellungen ist eng mit der Entwicklung des Datenschutzrechts verknüpft.

Bedingt durch die heranwachsende Informationsgesellschaft wurden personenbezogene Daten von bloßer Information zu einem wertvollen Wirtschaftsgut. Daten wurden das „neue Öl" einer informationsgetriebenen Gesellschaft. Damit einhergehend entstand in der zweiten Hälfte des 20. Jahrhunderts ein steigendes Bewusstsein am Schutz der eigenen Privatsphäre, sodass zunehmend gesetzliche Regelungen erforderlich wurden, um das Individuum vor (staatlichen) Eingriffen in sein Privatleben zu schützen. Im Rahmen des Europarates begannen in den 1970er Jahren Arbeiten an einem völkerrechtlichen Vertrag, um den Datenschutz rechtlich zu verankern. Parallel dazu fanden in den damaligen Mitgliedstaaten des Europarates, insbesondere in Deutschland und Österreich, erste Vorbereitungsarbeiten statt, um die elektronische Datenverarbeitung in gesetzliche Bahnen zu lenken und die Eingriffe staatlicher Behörden zu beschränken: Dies hatte zur Folge, dass das Grundrecht auf ▸

Datenschutz mittlerweile in fast allen Verfassungen der Mitgliedstaaten als klassisches Abwehrrecht vor staatlichen Eingriffen in die Privatsphäre verankert ist. Am Beginn dieser Entwicklung stand noch die Beschränkung der staatlichen Datensammlung im Vordergrund, gepaart mit der „informationellen Selbstbestimmung" des Einzelnen, wie es im sogenannten „Volkszählungsurteil" des deutschen Bundesverfassungsgerichts zum Ausdruck kommt. Der wirtschaftliche Wert personenbezogener Daten rückte in den letzten Jahrzehnten jedoch immer mehr in den Fokus und der Schutz der personenbezogenen Daten bekam eine neue – besondere Wichtigkeit.

Bei der genauen Betrachtung fällt auf, dass unterschiedliche Interessen einander diametral entgegenstehen: Der Schutz der eigenen Privatsphäre trifft auf ökonomische Interessen Dritter, die sich insbesondere in der (geldwerten) Verwertung von personenbezogenen Daten manifestieren. Es stellt sich die Frage, in welchen Fällen wirtschaftliche Interessen und in welchen Fällen Interessen des Individuums überwiegen können und sollen.

Diese ethischen Abwägungen sind auch im Datenschutz in erster Linie durch den Gesetzgeber zu treffen. Es ist in Gesetze zu gießen, welchen Interessen unter welchen Voraussetzungen Vorrang zu geben ist und in welchem Ausmaß in einer demokratischen Gesellschaft Eingriffe in den Schutz der Privatsphäre grundsätzlich als gerechtfertigt angesehen werden können.

Auf der Ebene der Vollziehung, auf der sich die nationalen Aufsichtsbehörden befinden, hat eine ethische Abwägung im Einzelfall zu erfolgen, etwa bei der Prüfung eines berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO.

Die am 25. Mai 2018 in Geltung getretene Datenschutz-Grundverordnung (DSGVO) ist die Materialisierung solch ethischer Abwägungen auf legislativer Ebene und erwies sich hierbei als Meilenstein für den Schutz personenbezogener Daten und als vorläufiger Endpunkt einer Entwicklung, die mit der Datenschutzkonvention des Europarates im Jahr 1981 begann. Der Europäische Wirtschaftsraum erfuhr durch ihre unmittelbare Anwendbarkeit nicht nur eine Vereinheitlichung rechtlicher Vorgaben im Hinblick auf Verarbeitungsvorgänge von personenbezogenen Daten, sondern es wurden auch europäische ethische Grundvorstellungen des Datenschutzes weiterentwickelt und gestärkt.

Zudem entfaltet die DSGVO durch ihren räumlichen Anwendungsbereich und die Bestimmungen des fünften Kapitels über „Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen" Relevanz und Vorbildwirkung über die Grenzen des Europäischen Wirtschaftsraumes hinaus. Dies zeigte sich beispielsweise bereits durch den Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 Abs. 3 DSGVO vom 23. Januar 2019 betreffend Japan[1]. Um eine solche Entscheidung zu erwirken, erfolgte durch Japan eine adäquate Annäherung der datenschutzrechtlichen Bestimmungen an die europäischen Standards der DSGVO.

Wirft man einen Blick in die DSGVO, so zeigt sich bereits in Art. 5 leg. cit., der die Grundsätze für die Verarbeitung personenbezogener Daten normiert, eine starke Verankerung der Datenethik. Sämtliche dort postulierten Grundsätze spiegeln fest verankerte Wertvorstellungen wider, die bei allen Datenverarbeitungen zu beachten sind.

In Art. 5 Abs. 1 lit. b DSGVO, dem Grundsatz der Zweckbindung, ist der ethische Hintergrund dieser Bestimmungen beispielsweise deutlich erkennbar. Der Mensch hat ein Interesse daran den Missbrauch seiner personenbezogenen Daten zu verhindern oder potentielle Gefahren zu vermeiden, indem für ihn erkennbar ist, zu welchen Zwecken seine Daten tatsächlich verarbeitet werden. Durch die Normierung des Zweckbindungsgrundsatzes darf ein Individuum erwarten, dass seine zu bestimmten Zwecken erhobenen Daten von einem Verantwortlichen oder Auftragsverarbeiter nur innerhalb dieses Rahmens verarbeitet werden. Die von dem europäischen Gesetzgeber hier vorgenommene ethische Abwägung zeigt sich darüber hinaus, da in der gleichen Norm die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zugelassen wird. Der europäische Gesetzgeber hat hier daher die Interessen des Individuums gegenüber der Allgemeinheit abgewogen und als Gesetz beschlossen.

Betrachtet man Art. 5 DSGVO, so kann man zu dem Schluss gelangen, dass die Grundsätze der DSGVO nicht nur auf der Datenethik beruhen, sondern vielmehr die Werte der Europäischen Union in Bezug auf Datenethik verkörpern. Art. 5 DSGVO sei hierbei jedoch lediglich als prominente Veranschaulichung genannt, da sich letztendlich in der gesam-

[1] Vgl. den Durchführungsbeschluss (EU) 2019/419 der Europäischen Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen.

te DSGVO Bestimmungen finden, die auf unseren ethischen Vorstellungen aufbauen.

Dies bedeutet, dass die in der DSGVO normierten Aspekte der Datenethik bei Verarbeitungsvorgängen von personenbezogenen Daten nicht nur von datenschutzrechtlichen Verantwortlichen und Auftragsverarbeitern einzuhalten sind, sondern umfassende Berücksichtigung erhalten: So haben auch die für die Überwachung der Anwendung dieser Verordnung zuständigen nationalen Aufsichtsbehörden und der Europäische Datenschutzausschuss (EDSA) jene in der DSGVO verankerten Grundsätze zu beachten und zu ihrer einheitlichen Anwendung im Europäischen Wirtschaftsraum ihren Beitrag zu leisten.

Dies bedeutet, dass sich die Rolle des EDSA und sein Handlungsradius im Wesentlichen auf die korrekte rechtliche Anwendung, Umsetzung und Auslegung der Bestimmungen der DSGVO bezieht. Diese Aufgabe nimmt der Ausschuss mittels der ihm übertragen Tätigkeiten gemäß Art. 70 DSGVO wahr, zu denen unter anderem Beratungstätigkeiten gegenüber der Europäischen Kommission, aber auch die Bereitstellung von Leitlinien, Empfehlungen und Stellungnahmen zählen.

Um seine Aufgabe effizient und effektiv erfüllen zu können und entsprechende Dokumente für eine einheitliche Anwendung der DSGVO bereitzustellen, wird innerhalb des EDSA für die jeweiligen rechtlichen Anwendungsfälle die hierfür thematisch relevante Expertenuntergruppe des Ausschusses befasst. An dieser Stelle sei erwähnt, dass der Ausschuss derzeit zwar über 13 Expertenuntergruppen verfügt, sich unter diesen jedoch keine eigenständige Datenethik-Expertenuntergruppe wiederfindet. Dies einerseits deshalb, weil sich – wie bereits festgehalten – die Rolle des EDSA im Wesen auf die DSGVO und damit einhergehende juristische und technische Aspekte bezieht. Der Ausschuss widmet sich daher weniger konkreten Diskussionen der Datenethik, sondern arbeiten dessen Expertenuntergruppen mit einem juristischen Fokus. Sämtliche Dokumente des Ausschusses werden im Lichte der rechtlichen Bestimmungen der DSGVO erarbeitet und sind letztlich als nähere Konkretisierungen beziehungsweise Auslegungshilfen dieser heranzuziehen. Andererseits erweist sich eine eigenständige Datenethik-Expertenuntergruppe derzeit aus Sicht der Autorinnen auch nicht als erforderlich und wäre im strukturellen Gefüge der bestehenden Expertenuntergruppen schwierig einzugliedern, da ethische

Grundsätze der DSGVO inhärent und daher von allen Expertenuntergruppen zu berücksichtigen sind.

Darüber hinaus werden, aufgrund der Zusammensetzung des Ausschusses aus den Leitern und Leiterinnen der nationalen Aufsichtsbehörden, naturgemäß auf sämtlichen Ebenen des EDSA die unterschiedlichsten, relevanten Problemstellungen diskutiert und behandelt, die auch Aspekte der Datenethik umfassen. Der EDSA agiert auch hier im Rahmen seiner Zuständigkeit und das Ergebnis solcher Diskussionen findet sich in den beschlossenen Dokumenten des Ausschusses wieder.

Sämtliche Dokumente des Ausschusses dienen den unabhängigen nationalen Datenschutzbehörden bei der Anwendung der DSGVO als Richtschnur und den Stakeholdern als Maßstab für die einheitliche Anwendung der DSGVO im Europäischen Wirtschaftsraum.

Dies wurde insbesondere während der COVID-19-Pandemie deutlich sichtbar, die den Datenschutz ins Rampenlicht rückte und seine Relevanz für die Bevölkerung vor Augen führte. So wurden von einem Tag auf den anderen die unterschiedlichsten kritischen Fragen heftig diskutiert, wie beispielsweise:

- Ist die Verwendung von sogenannten Contact-Tracing-Apps zulässig und wenn ja, unter welchen Voraussetzungen? ▶

[2] Vgl. EDPB Annual Report 2019, S 44-47; https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2019_en.pdf

- Unter welchen Umständen dürfen meine personenbezogenen Daten für die Entwicklung einer Impfung gegen das Coronavirus verwendet werden?
- Welche konkreten Voraussetzungen müssen gegeben sein, damit meine Betroffenenrechte gemäß Art. 23 DSGVO beschränkt werden dürfen?

All diese Fragen enthalten naturgemäß auch datenethische Aspekte, und die Wertvorstellungen einer demokratischen Gesellschaft geraten damit auf den Prüfstand.

Der EDSA nahm sich unter anderem der Beantwortung der oben angeführten Fragen an und konnte in dieser kritischen Zeit unter Beweis stellen, dass es sich bei dem Ausschuss um ein flexibles neues EU-Gremium handelt und die DSGVO ein krisentaugliches gesetzliches Gerüst ist. Die Erarbeitung entsprechender Leitlinien und Stellungnahmen gelang und ermöglichte rasch Klarheit auf europäischer Ebene über Verarbeitungsvorgänge personenbezogener Daten während der COVID-19-Pandemie zu schaffen.

Um auf das Beispiel der Contact-Tracing-App zurückzukommen, hielt der EDSA unter anderem in seinen Leitlinien fest, dass Standortdaten für eine solche Applikation nicht erforderlich und stattdessen sogenannte Proximity-Daten zu verwenden seien, also Daten, die keinen Rückschluss auf den Standort einer Person zulassen, sondern lediglich die Nähe zu einer anderen Person oder ihren Geräten aufzeigen.

Die Rolle des EDSA zeigt sich in diesen Leitlinien auch gut in seiner Beantwortung der Frage, ob bei der Speicherung personenbezogener Daten im Zuge einer Contact-Tracing-App ein zentraler oder dezentraler Ansatz zu wählen ist. Der EDSA entschied, dass beide Ansätze aus datenschutzrechtlicher Sicht grundsätzlich zulässig seien, hielt jedoch fest, dass eine dezentrale Speicherung im Allgemeinen eher dem Grundsatz der Datenminimierung entspreche.

Die COVID-19-Pandemie führte auf Ebene des EDSA zudem nicht nur zu Leitlinien und an die Öffentlichkeit gerichteten Stellungnahmen des Ausschusses, sondern auch zu der bereits erwähnten, konkreten Beratungstätigkeit gegenüber der Europäischen Kommission: So wurde der Ausschuss im Zuge der Erarbeitung der Leitlinien der Kommission zum Datenschutz bei Mobil-Apps zur Unterstützung der Bekämpfung der COVID-19-Pandemie konsultiert. Die Stellungnahme des Ausschusses fand hierbei im entsprechenden Dokument der Kommission Berücksichtigung.

Die COVID-19-Pandemie hat auch aus diesen Gründen Auswirkungen auf Fragen des Datenschutzes und der Datenethik und verdeutlicht, wie weitreichend diese Themenbereiche sind.

Bestimmungen des Datenschutzes und insbesondere die DSGVO behindern Maßnahmen im Kampf gegen die COVID-19-Pandemie nicht, der Kampf gegen übertragbare Krankheiten ist ein wichtiges Ziel, das auf bestmögliche Weise unterstützt werden muss. Die Eindämmung der Ausbreitung von Krankheiten und der Einsatz moderner Techniken, um dies zu verwirklichen, liegen daher im Interesse der Bevölkerung. Auch unter diesen Umständen ist der Schutz der personenbezogenen Daten von betroffenen Personen zu gewährleisten.[4] Der technische Fortschritt wird daher durch das Datenschutzrecht nicht aufgehalten oder behindert, die DSGVO stellt vielmehr einen europaweit vereinheitlichten Standard für den Schutz personenbezogener Daten dar, der einzuhalten ist.

[3] Vgl. die am 21. April 2020 angenommenen Leitlinien 04/2020 des EDSA für die Verwendung von Standortdaten und Tools zur Kontaktnachverfolgung im Zusammenhang mit dem Ausbruch von COVID-19.

[4] Vgl. EDPB Statement on the processing of personal data in the context of the COVID-19 outbreak, adopted on 19 March 2020.

Über die Autorinnen

Mag. Barbara Chlopcik
ist juristische Referentin der Österreichischen Datenschutzbehörde. Seit 2019 ist sie auf internationaler Ebene in der Vorsitzkoordination des Europäischen Datenschutzausschusses tätig und leitet darüber hinaus seit Mai 2020 das internationale Büro innerhalb der Behörde.

Dr. Andrea Jelinek
ist seit 25. Mai 2018 Vorsitzende des Europäischen Datenschutzausschusses und seit 2014 Leiterin der Österreichischen Datenschutzbehörde.

▶ https://edpb.europa.eu/edpb_de

DIGITALE ETHIK ALS REFLEXIONSPROZESS

Sollen Datenschutzbeauftragte zugleich Digitalethiker sein?

Von Dr. Nikolai Horn

Einleitung

Digitale Ethik gewinnt gegenwärtig nicht nur auf der zivilgesellschaftlichen, sondern auch auf der staatlichen und unternehmerischen Ebene immer mehr an Bedeutung. Ob im Rahmen der von den Regierungen und Parlamenten eingesetzten Ethikkommissionen, „Corporate Digital Responsibility" (CDR) Ansätzen von Unternehmen oder der Ausarbeitung von ethischen Leitfäden durch die Zivilgesellschaft – ethische Auseinandersetzungen mit der Digitalisierung sind mittlerweile in ihrer Notwendigkeit erkannt und werden zunehmend selbstverständlich. Dabei ist allerdings nicht immer klar, ob die einzelnen Akteure darunter dasselbe verstehen. Um eine Antwort auf die Frage geben zu können, ob die Datenschutzbeauftragten zugleich Digitalethiker sein sollen oder können, muss daher zunächst geklärt werden, was eigentlich unter „Ethik" im Allgemeinen und unter einer „Digitalen Ethik" im Besonderen zu verstehen ist. Wo liegt die Grenze zwischen Ethik und Recht? Wie hängen diese Bereiche zusammen? Wie sind Prinzipien begründet, mit denen wir ethisch urteilen? Welchen Stellenwert soll schließlich eine „Digitale Ethik" bei der Etablierung von datengestützten Innovationen innerhalb von Organisationen haben? Um diese Fragen zu beantworten, wird im vorliegenden Aufsatz zunächst auf die Bedeutung des Begriffs „Ethik" eingegangen und die Grundlagen von ethischen Diskursen verdeutlicht, um anschließend auf die Rolle von Datenschutzbeauftragten für digitalethische Diskurse einzugehen und abschließend mögliche Herangehensweisen bei digitalethischen Reflexionen vorzustellen.

1. Was ist „digitale Ethik"?

Ob Gutachten der Datenethikkommission der Bundesregierung, Vorschläge zu ethischen Leitlinien für die Künstliche Intelligenz der EU-Kommission oder die Zwischenergebnisse der KI-Enquete des Deutschen Bundestages – Digitale Ethik ist längst kein Randphänomen der praktischen Philosophie mehr, sondern ein fester Bestandteil des politischen Diskurses in einer digitalen Gesellschaft. Dennoch scheint nicht immer klar zu sein, was eine (digital)ethische Fragestellung eigentlich ist und wie sie sich von den rechtlichen oder ▸

digitalpolitischen Fragen abgrenzt. So ist es beispielsweise bei der Auseinandersetzung mit Datenrechten und Datenpflichten im Gutachten der Datenethikkommission der Bundesregierung[1] nicht immer leicht abzugrenzen, wann es dort um ethische Reflexionen geht, und wann es sich um rechtsdogmatische Überlegungen handelt. Es liegt womöglich in der Natur der Sache, dass hier eine klare Abgrenzung nur schwerfallen kann. Dennoch bieten die gegenwärtigen Diskussionen über die Ethik des Digitalen immer wieder den Anlass (etwa bei der Diskussion um die „Corona-App") sich über den Bedeutungsgehalt der „Digitalen Ethik" zu vergewissern. Beispielhafte Fragestellungen sind: Wie grenzt sich die Ethik von der Moral und von dem Recht ab? Was ist eigentlich eine *digitale* Ethik? Wann werden die (digital)ethischen Auseinandersetzungen in der Regel relevant? Warum ist eine ethische Reflexion über die Herausforderungen der Digitalisierung wichtig?

Ethik ist zunächst eine philosophische Disziplin, welche dem Bereich der „praktischen Philosophie" zugeordnet wird und der Frage nach dem „guten Handeln" nachgeht – oder, mit Kant ausgedrückt, der Frage „Was soll ich tun?".[2] Während die „Moral" gesellschaftliche Normen, sittliche Regeln, Gebräuche, kulturelle Gepflogenheiten und gesellschaftliche Konventionen zum Gegenstand hat (beispielsweise politisch korrekte Ausdrucksweisen, „europäische Werte", ungeschriebene Verhaltensregeln und so weiter), macht die Ethik die Begründung dieser Grundsätze selbst zum Gegenstand der Betrachtung. Die Ethik beschäftigt sich dabei mit der Frage, welche moralische Ansichten wann und warum gelten. Sie sucht also nach allgemeinen Prinzipien des „guten Handelns" (wie zum Beispiel dem „Kategorischen Imperativ"), mit denen sich bestimmte gesellschaftliche Normen und individuelle Handlungsgrundsätze begründen lassen. Während beispielsweise der Nicht-Kauf eines SUV-Fahrzeuges der Gegenstand einer bestimmten moralischen Haltung sein kann, wäre der Gegenstand einer ethischen Reflexion eine Frage nach dem Prinzip, wie man in einer hochtechnologisierten Konsumgesellschaft individuelle Verantwortung für die Umwelt übernehmen kann.

Eine *angewandte* Ethik beschäftigt sich ihrerseits mit der Anwendung einzelner ethischer Prinzipien oder Normen auf konkrete bereichsspezifische Problemfälle. So setzt sich beispielsweise die Medizinethik mit der Frage nach der Zulässigkeit der Sterbehilfe oder die Bioethik mit den Grenzen der Genforschung auseinander. Die Digitale Ethik, als angewandte Ethik, greift ihrerseits bestimmte Phänomene des Digitalisierungsprozesses auf und fragt nach dem Guten und Richtigen im Datenzeitalter. Aus der Perspektive der Digitalethik wird beispielsweise gefragt:

- Inwiefern können digitale Technologien die Freiheit und Selbstbestimmung der Menschen beeinträchtigen?
- Welche Entscheidungen können und sollten einem datenverarbeitenden algorithmischen System übertragen werden und welche besser nicht?
- Wer trägt die Verantwortung für fehlerhafte datengestützte Entscheidungen?
- Rechtfertigt die Sorge um die öffentliche Sicherheit und Gesundheit eine umfassende Datenüberwachung?
- Ist eine automatische, auf digitalen Technologien beruhende Sanktionierung von Rechtsverstößen mit unseren demokratischen Grundwerten vereinbar?

Bereits die Formulierung solcher und ähnlicher Fragen ist eine Form der angewandten Ethik, die man auch als „Digitale Ethik" bezeichnen kann.

Digitalethische Fragen werden meist dann relevant, wenn:

- der Umgang mit bestimmten technologischen Neuerungen (z.B. bestimmte algorithmische Entscheidungen in autonomen Fahrzeugen) noch nicht umfassend rechtlich geregelt ist;
- bestimmte Rechtsregelungen weite Interpretationsspielräume aufweisen (z.B. wie eng oder wie breit „erheblicher Eingriff" oder „menschliche Intervention" in der DSGVO auszulegen ist);
- die Folgen bestimmter technologischer Entwicklungen schwer abzuschätzen sind (z.B. der Einsatz der Robotik für die Zukunft der Arbeitswelt);
- es bei der Ausgestaltung digitaler Systeme um mehr als „bloß" um rechtliche Mindestanforderungen geht (z.B. bei der Bereitstellung bestimmter „Privacy Enhancing Technologies" (PET));
- durch die Anwendung digitaler Produkte bestimmte ethische Zielkonflikte entstehen (z.B.

[1] Gutachten der Datenethikkommission der Bundesregierung, S. 79 ff. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=C229DDDDE93169EE3AAC037F91467136.2_cid373?__blob=publicationFile&v=6

[2] Horn, Nikolai: „Grundlagen der digitalen Ethik - Eine normative Orientierung in der vernetzten Welt", Denkimpuls der AG Ethik der Initiative D21, 2017. S. 1 f. URL: https://initiatived21.de/app/uploads/2017/08/01_denkimpulse_ag-ethik_grundlagen-der-digitalen-ethik.pdf

Selbstbestimmung von Patienten versus algorithmische Entscheidung eines Pflegeroboters).

In all diesen Fällen reflektiert die Digitalethik über Sachverhalte, die das gesellschaftliche Selbstverständnis betreffen und eine breite gesellschaftliche Akzeptanz erfordern. Diese Reflexion ist dabei als ein Prozess zu verstehen. Ethik als Reflexionsprozess identifiziert eine bestimmte Problemsituation, leitet daraus konkrete ethische Fragestellungen ab, stellt unterschiedliche Perspektiven auf den konkreten Problemfall vor und arbeitet anhand eines normativen Maßstabes bestimmte Lösungswege aus.

2. Autonomieprinzip und digitale Verantwortung

2.1 Der Maßstab digitalethischer Reflexion und das verfassungsimmanente Menschenbild

Der Maßstab einer (digital)ethischen Reflexion ist im Grunde genommen ein bestimmtes Menschen- und Weltbild. Denn aus dem Verständnis dessen, was eigentlich den Menschen als solchen ausmacht, lassen sich sowohl bestimmte ethische Normen ableiten, als auch Maßstäbe für das „gute" Handeln festlegen.[3] Geht man beispielsweise vom Menschenbild eines kollektivistischen Staates aus, demgemäß das Wohl der „Gemeinschaft" grundsätzlich die Selbstbestimmung des Einzelnen überwiegt, so lassen sich daraus ganz andere Auffassungen über das „Gute" und das „Richtige" (etwa bei Massenüberwachung) ableiten, als wenn man die individuelle Selbstbestimmung grundsätzlich als das höchste Gut begreift. Geht man bei der Beziehung Individuum-Staat von einem Kooperationsverständnis aus (wie es beispielsweise in skandinavischen Ländern oder auch in Südkorea stark verankert ist), lassen sich im Zuge einer ethischen Reflexion gegebenenfalls andere Konsequenzen ableiten, als in einem Kulturraum wie dem deutschen, in dem ein geschichtlich bedingtes Grundmisstrauen gegenüber dem Staat vorherrscht.

Das Menschenbild des Grundgesetzes geht jedenfalls von einem Bürgerverständnis aus, das das eigenverantwortliche Individuum ins Zentrum stellt, welches in eine Gemeinschaft eingebunden ist, in der jeder über eine bei anderen gleich zu achtende Würde verfügt.[4] Es ist ein Menschenbild, nach dem das Individuum einerseits selbstbestimmt, andererseits verantwortungsbewusst gegenüber seinen Mitmenschen ist. Für eine digitalethische Auseinandersetzung könnte der Rückgriff auf das freiheitliche Menschenbild des Grundgesetzes jedenfalls ein gutes und bewährtes Grundprinzip darstellen, mit dessen Hilfe über bestimmte Herausforderungen der Digitalisierung reflektiert werden kann.

Das dem verfassungsimmanenten Menschenbild zugrundeliegende Autonomieprinzip des Individuums ist ein ethisches Prinzip, das insbesondere seit den Anfängen der Aufklärung mehrfach als Grundlage für die Begründung von Freiheitsrechten herangezogen wurde. Bereits der Renaissancehumanist Pico della Mirandola erklärt die Freiheit und Würde des Menschen aus dem Vermögen, kraft seiner Vernunft die Welt nach eigener Vorstellung schöpferisch zu gestalten.[5] Spätestens seit den „Kritischen Schriften" von Immanuel Kant wird das Menschenbild der Aufklärung von der normativen Annahme seiner Vernünftigkeit und Freiheitlichkeit her bestimmt. Daraus wird das für das Verständnis der Menschenwürde konstitutive Prinzip begründet, dass der Mensch eigene Handlungen und sein Leben frei nach eigener Vorstellung zu gestalten vermag. Die damit begründete Souveränität des Individuums bedeutet, jederzeit die Hoheit und Verantwortung über den eigenen Lebensentwurf zu haben.

Auf die Nutzung der Informationstechnik angewendet bedeutet dieses Prinzip, auch bei der Nutzung der Informationstechnologie diese Hoheit jederzeit zu behalten. Beispielsweise darüber, was mit den in sozialen Netzwerken geteilten Daten wirklich passiert. Von dieser normativen Grundlage ausgehend kann die „digitale Autonomie" aus der ethischen Perspektive daher nichts anderes bedeuten, als Selbstbestimmung über das Daten-Abbild ▶

[3] Ebd. S. 4.

[4] vgl. Di Fabio, Udo: Die Zukunft der Bürgergesellschaft – die Aufgabe der Bürgerstiftungen. Berlin, 23.03.2012.

[5] della Mirandola, Giovanni Pico: Über die Würde des Menschen. Hamburg 1990. S. 5 f.

seiner Selbst, die Hoheit des Individuums über algorithmische Systeme sowie die Freiheit, in eigenem Lebensentwurf nicht durch eigene Datenspuren und durch die von Dritten erstellten Persönlichkeitsprofile „prädeterminiert" zu sein. Hierauf zielt letztlich auch das rechtliche Konzept der „informationellen Selbstbestimmung". Denn es geht hierbei um mehr als nur um die Schonung der Privatsphäre als einen Rückzugsraum des Individuums. Es geht vor allem um die Möglichkeit einer aktiven, selbstbestimmten Gestaltung der eigenen Lebenswelt unter der Nutzung digitaler Technologien.

2.2 Digitale Verantwortung von Unternehmen und Staat

Aus diesem Grund geht es bei der Anwendung des normativen Prinzips der Autonomie auf die Verarbeitung von personenbezogenen Daten um mehr als „nur" um den rechtlichen Datenschutz, der ein Fundament für die informationellen Selbstbestimmungsmöglichkeiten des Individuums darstellt. Auf diesem Fundament muss das Haus aber noch gebaut werden. Die Hoheit des Individuums über die Verwendung seiner personenbezogenen Daten und Informationen impliziert nämlich auch die praktische Befähigung, sich mit entsprechenden Kenntnissen und geeigneten technologischen Instrumenten reflektiert und selbstbestimmt in der „Datenwelt" zu bewegen.[6] Für diese Befähigung stellt die rechtliche Komponente der Datenschutz-Grundverordnung zwar eine Grundlage dar, die gesellschaftliche Komponente des verantwortungsbewussten Umgangs mit personenbezogenen Daten der Bürgerinnen und Bürger durch Unternehmen und staatliche Institutionen spielt jedoch eine nicht minder wichtige Rolle. Genauso wie die Bildungskomponente der Vermittlung von Datenschutzkompetenzen sowie die technologische Komponente der Nutzung von den die Selbstbestimmung fördernden Technologien, welche den Nutzerinnen und Nutzern praktische Instrumente an die Hand geben, um ihre digitalen Freiheitsrechte auszuüben und den Machtasymmetrien entgegenzuwirken.

Der Staat und die Unternehmen tragen dabei neben den Rechtspflichten auch eine gesellschaftliche Verantwortung. Um Bruchstellen zwischen dem Anspruch auf die Achtung der digitalen Selbstbestimmungschancen und der in Wirklichkeit erfahrenen Ohnmacht der Einzelnen gegenüber datenverarbeitenden Institutionen zu überwinden, benötigt es „Vertrauensanker", welche einen fairen Umgang mit personenbezogenen Daten garantieren und auf die sich die Menschen verlassen können. Mit „Vertrauensanker" sind dabei sowohl Expertisen von vertrauenswürdigen Institutionen, wie beispielsweise den Aufsichtsbehörden oder Privatinitiativen (z.B. MyData-Initiative oder Chaos Computer Club) gemeint, als auch der Einsatz von „Privacy Information Management Systems" (PIMS), welche auf der technologischen Ebene dem Individuum ein Instrument für die Steuerung der Verwendung von personenbezogenen Daten zur Verfügung stellen.

Das Konzept einer Corporate Digital Responsibility (CDR) könnte dabei ein wichtiges Instrument sein, um ethische Reflexionsprozesse auf unterschiedlichen Ebenen institutionell zu verankern. CDR steht für verantwortungsvolles unternehmerisches Handeln nach innen und außen bei der Ausübung digitaler Geschäftsprozesse, der Gestaltung von digitalen Services und Produkten sowie den damit verbundenen (Daten-)Austauschbeziehungen gegenüber Mitarbeitenden, allen Marktpartnern und der Gesellschaft.[7] In der Praxis können CDR-Strategien unterschiedlich ausgestaltet und gelebt werden – von Jahresreports über Investitionen und Maßnahmen des Unternehmens in Sachen Datenschutz, über branchenspezifische selbstverpflichtende Maßnahmen im Bereich der Digitalisierung und des Datenmanagements bis hin zu konkreten Mitarbeiterschulungen und dem Einsatz von Transparenztools zur Nutzung personenbezogener Daten der Kunden.[8]

Als Vertrauensanker kommen aber nicht nur CDR-Ansätze von Unternehmen in Frage, sondern auch der Staat als Garant der Einhaltung von Datenschutzbestimmungen und als Förderer digitaler Selbstbestimmung. Eine „Public Digital Responsibility" sollte dabei als ein Teil der öffentlichen Daseinsvorsorge aufgefasst werden. Denn die Digitalisierung des öffentlichen Raums im Sinne des Ausbaus öffentlicher Infrastruktur, digitaler Kultur-, Bildungs- und Verwaltungsangebote kann nur dann im Sinne von Bürgerinnen und Bürgern sein, wenn ihre informationellen Selbstbestimmungschancen dadurch gestärkt und eventuell sogar ausgeweitet werden.[9] Die digitale Autonomie im Sinne einer „digitalen Daseinsvorsorge" wird gefördert, wenn die Einhaltung von Datenschutzregeln sichergestellt, technologische Instrumente für ein selbstbestimmtes Handeln im digitalen Raum bereitgestellt und digitale Kompetenzen vermittelt werden.

[6] Vgl.: Horn, Nikolai / Stecher, Björn: Denkimpuls Innovativer Staat: „Datensouveränität – Datenschutz neu verstehen", Initiative D21 (Hg.), Mai 2019. URL: https://initiative21.de/app/uploads/2019/05/denkimpuls_datenschutz_neu_verstehen.pdf

[7] Jänig, Jens-Rainer: „Kurzeinführung – Corporate Digital Responsibility". Vortrag, 21.06.2018. Berlin, Arbeitsgruppe Ethik, Initiative D21

[8] Horn, Nikolai / Stecher, Björn: Denkimpuls Innovativer Staat: „Datensouveränität – Datenschutz neu verstehen", Initiative D21 (Hg.), Mai 2019, S. 6

[9] Ebd., S. 7

Ob durch den Staat oder durch Unternehmen – die Auseinandersetzung mit ethischen Fragen, wie sie oben im Kapitel 1. beschrieben wurden, ist integraler Bestandteil verantwortungsvoller Gestaltung des digitalen Transformationsprozesses. Staatliche und private Einrichtungen sollen durch ethische Reflexionen die Folgen des Einsatzes bestimmter datenverarbeitender Technologien für die Mitarbeitenden und für die Bevölkerung frühzeitig antizipieren und Auswirkungen auf das für unsere Gesellschaft konstitutive Menschenbild selbstkritisch hinterfragen. Ein solcher Prozess soll dabei jedoch kein Feigenblatt sein, sondern genauso ernstgenommen werden, wie die Abwägung von Investitionsmaßnahmen für den Unternehmenserfolg oder wie die politische Folgenabschätzung beim Handeln der Exekutive.

Der ethische Reflexionsprozess ist dabei keine Einbahnstraße – die Institutionalisierung des ethischen Reflexionsprozesses muss unterschiedliche Instanzen, Berufsgruppen und interdisziplinäre Perspektiven einbeziehen, um sich argumentationsförmig und konstruktiv mit ethischen Herausforderungen auseinanderzusetzen.[10] Außerdem soll im Sinne eines gesamtgesellschaftlichen Diskurses die Einbeziehung zivilgesellschaftlicher Akteure, der Wissenschaft und der digitalpolitischen Think Tanks von vornherein in Erwägung gezogen werden.

3. Datenschutzbeauftragte – „Innovationsausbremser“ oder „digitale Guides“?

Welche Rolle können die Datenschutzbeauftragten im ethischen Reflexionsprozess einnehmen? Die Aufgabe von Datenschutzbeauftragten, die Verantwortlichen bei der Auslegung und der Umsetzung von datenschutzrechtlichen Bestimmungen zu unterstützen, ist zunächst auch ohne „Ethik“ nicht trivial. Diese Aufgabe wird umso wichtiger, wenn nicht nur Prozess-Know-how, sondern auch die Datenquantität und insbesondere -qualität über den Geschäftserfolg entscheidet. Mit den steigenden Anforderungen an die Rechtmäßigkeit der Datenverarbeitung und an die Sicherheit von Verarbeitungsprozessen steigt dabei auch die Komplexität der Aufgabenerfüllung im Bereich „Data Governance“ bei der Modellierung von Organisationsprozessen, bei der Ausgestaltung von IT-Systemen und Applikationen sowie bei den Mitarbeiterschulungen. Ist es vor diesem Hintergrund überhaupt zumutbar, den Datenschutzbeauftragten auch noch die Zuständigkeit für die „Ethik“ aufzubürden?

Erschwerend kommt hinzu, dass dem Datenschutz im Allgemeinen und den Datenschutzbeauftragten im Besonderen leider weiterhin oft das Klischee anhaftet, „Innovationsausbremser“ zu sein. Das negative Bild entsteht insbesondere dann, wenn die Datenschutzbeauftragten nicht von vornherein in die Konzeption digitaler Prozesse und Anwendungen miteingebunden werden und ihre Einschätzungen erst gegen Ende des Entwicklungsprozesses, also wenn viele Tatsachen bereits vollendet sind, einfließen. An dieser Stelle erscheint wohl jeder Datenschutzhinweis automatisch als „Ausbremser-Argument“.

Ihre frühzeitige Einbindung als qualifizierte Experteninnen und Experten in den gesamten Data-Governance-Lebenszyklus könnte dagegen sehr gut dazu beitragen, dass sie von der Managementebene vielmehr als Begleiter der Digitalisierung wahrgenommen werden, die innovative Lösungen ermöglichen, das Unternehmensimage schützen und das Kundenvertrauen ausbauen. Dazu ist mitunter ein Perspektivenwechsel erforderlich, der auch die Digitalisierung als einen Prozess, den Datenschutz als Kunden- und Mitarbeiterbefähigung und die Datenschutzbeauftragten als „Digitale Guides“ begreift.

Das gleiche gilt für die Auseinandersetzung mit digitalethischen Fragen. Immer öfter wird inzwischen das negative „Innovationsausbremser“-Bild des Datenschutzes auch auf die Ethik übertragen.[11] Wenn die Datenschutzbeauftragten zusätzlich auch noch für „ethische Bedenken“ zuständig sein würden, könnte sich das negative „Ausbremser“-Bild weiter verfestigen. Aber auch hier gilt – eine frühzeitige Beschäftigung mit digitalethischen Fragen und die Einbeziehung der digitalethischen Reflexionen und Überlegungen in den gesamten Data-Governance-Lebenszyklus muss als ein Prozess begriffen werden. Ethik, genauso wie der Datenschutz, ist ein Reflexionsprozess – hier über datenschutzrechtliche Aspekte, da über die normativ-ethische Aspekte – und kein „Bedenkentum“.

Aufgrund ihrer intimen Kenntnis der technischen und rechtlichen Rahmenbedingungen, des technologischen und datenschutzrechtlichen Reifegrades ihrer Institution sowie der genutzten Anwendungen und bestehender Organisationsstrukturen haben die Beauftragten auf der methodischen ▸

[10] Vgl., Armin Nassehi: „Die letzte Stunde der Wahrheit. Kritik einer komplexitätsvergessenen Vernunft“, Hamburg 2019, S. 207 f

[11] Vgl. dazu Interview mit der Staatsministerin für Digitales Dorothee Bär „Zu satt für die Digitalisierung“, in: Frankfurter Allgemeine Zeitung“ vom 31.10.2019. URL: https://www.faz.net/aktuell/wirtschaft/digitec/dorothee-baer-zu-satt-fuer-die-digitalisierung-16459998.html

Ebene einen der besten Zugänge, um digitalethische Fragen im konkreten Geschäftskontext anzugehen. Denn bei der Beurteilung von Anforderungen und Normen zum Umgang mit Daten im Zuge einer umfassenden Data Governance werden mit Hilfe von Datenschutzbeauftragten ganz konkrete Zuständigkeiten, Rollen und Rechte sowie Prozesse und Methoden im Umgang mit Daten definiert. Dadurch gewinnen die Datenschutzbeauftragten einen umfassenden Einblick in den gesamten Data-Governance-Lebenszyklus und eignen sich daher in einer besonderen Weise, um auch digitalethische Reflexionen als Begleiter zu betreuen.

Sollen nun die Datenschutzbeauftragten zugleich Digitalethiker sein? So einfach ist die Antwort nicht. Obwohl sie, wie oben beschrieben, aufgrund ihres methodischen Wissens eine hohe Kompetenz für die Auseinandersetzung mit ethischen Fragen mitbringen, besteht ihre primäre und aufwandsintensive Aufgabe immer noch in der Sicherstellung der datenschutzrechtlichen Konformität. Die „digitale Ethik" soll dabei nicht zum „lästigen Anhängsel" in der Zuständigkeit eines *einzelnen* Verantwortlichen im Unternehmen werden. Richtig verstanden soll sie vielmehr als ein institutionsübergreifender Reflexionsprozess aufgefasst werden. Bei diesem Prozess können die Datenschutzbeauftragten aufgrund ihrer Kompetenzen eine sehr wichtige, aber eben niemals die alleinige Rolle spielen. Vertreter der Geschäftsführung, der Entwicklungsabteilungen, der Betriebsrat, die Gleichstellungsbeauftragten, einzelne Mitarbeiterinnen und Mitarbeiter sowie gegebenenfalls unabhängige externe Expertinnen und Experten sollen bei einem ernstgemeinten ethischen Reflexionsprozess ebenfalls miteinbezogen werden. Denn die ethische Reflexion als Suche und Anwendung von normativen Prinzipien auf bereichsspezifische Probleme in einem ganz bestimmten Geschäftskontext hat einen Diskurscharakter.

Beim digitalethischen Diskurs können die Datenschutzbeauftragten vor allem dazu beitragen, dass die Diskursteilnehmer und -teilnehmerinnen die rechtlichen Mindestanforderungen, den Status quo ihrer gegenwärtigen Umsetzung, die Interpretationsspielräume und gegebenenfalls „weiße Flecken" der Rechtsregulierung im konkreten Anwendungsbereich sowie die technologischen Anforderungen besser verstehen. Dadurch werden sie mit Hilfe von Datenschutzbeauftragten befähigt, den Ausgangspunkt für eine ethische Reflexion, für die Zielsetzung im Kontext der konkreten digitalen Umgebungen sowie den Weg zu ethisch vertretbaren digitalen Lösungen informiert und sachgerecht beurteilen zu können. Auch in ethischen Fragen eignen sich die Datenschutzbeauftragten daher bestens als „Digitale Guides".

4. Leitfaden für ethische Reflexionsprozesse

Wie kann ein ethischer Reflexionsprozess in der Praxis umgesetzt werden? Für die Auseinandersetzung mit philosophischen und ethischen Fragestellungen ist ein Abend mit Kerzen und Wein sicherlich der eleganteste Weg. Um eine kontextbezogene Anwendung von ethischen Prinzipien auf bereichsspezifische Fragestellungen innerhalb von öffentlichen oder privaten Einrichtungen zu entwickeln, ist allerdings eine systematische Vorgehensweise erfolgsversprechender. Einen Königsweg gibt es dazu nicht, denn ethische Reflexionen sind meist sehr anwendungsspezifisch. Aus diesem Grund werden im Folgenden exemplarisch zwei Ansätze präsentiert, wie man bei der Auseinandersetzung mit digitalethischen Fragen grundsätzlich vorgehen könnte. Es handelt sich dabei zum einen um eine Matrix mit ethischen Zielkonflikten der AG Ethik der Initiative D21 und zum anderen um den jüngst erschienenen, von dem unabhängigen Think Tank iRights.Lab in Kooperation mit der Bertelsmann-Stiftung ausgearbeiteten, „Praxisleitfaden zu den Algo.Rules"[12].

Die AG Ethik der Initiative D21 geht beispielsweise von ethischen Zielkonflikten aus, die bei der Anwendung von digitalen Produkten entstehen können.[13] Der Ausgangspunkt dieser Herangehensweise ist die Verifizierung von konkreten ethischen Zielkonflikten und ein anschließender Diskurs über mögliche Wege ihrer Behebung. Es werden generisch mögliche ethische Zielkonflikte beschrieben, die in einem Diskurs über konkrete Anwendungsszenarien verifiziert und anschließend auf der technologischen Ebene angegangen werden. Die Zielkonflikte werden ausgehend von Schutzsphären und möglichen konkurrierenden Werteabwägungen her bestimmt und die Anwenderinnen und Anwender eingeladen, innerhalb ihrer spezifischen Anwendungsszenarien in einem Diskurs mögliche Zielkonflikte zu finden und sich über ihre Auflösung anhand von Interessens- und Folgeabwägungen zu verständigen. Als Vorlage dient eine Tabelle, anhand derer ein ethischer Reflexionsprozess gestaltet werden kann:

[12] https://irights-lab.de/praxisleitfaden/

[13] Lena-Sophie Müller / Nicolai Andersen: Warum wir uns mit Digitaler Ethik beschäftigen sollten – Ein Denkmuster. Berlin, 2017 URL: https://initiative21.de/app/uploads/2017/08/01-2_denkimpulse_ag-ethik_digitale-ethik-ein-denkmuster_final.pdf

Denkmuster Digitale Ethik

iRights.Lab — Initiative D21

		Zielkonflikte	Datifizierung (Datenerhebung, -auswertung, -interpretation)	Automatisierung, algorithmische Entscheidungen	Vernetzung / Virtualisierung	Mensch-Maschine-Interaktion
Folgen-Abwägung	Interessen-Abwägung	Personalisierung vs. Privatsphäre	Smart Learning Environments optimieren den Lernprozess vs. sammeln persönlicher Daten der Nutzer		Daten von Wearables werden an Versicherungen übermittelt um individuelle Angebote zu erstellen vs. Schutz der Daten	
Folgen-Abwägung	Interessen-Abwägung	Zugänglichkeit vs. Privatsphäre	Sammlung von Connected Car Daten optimiert Verkehrswege vs. Erstellung von Bewegungsprofilen		Smart Homes sorgen dafür das Energie eingespart wird vs. Erstellung von Nutzungsprofilen	
Folgen-Abwägung	Interessen-Abwägung	Benutzerfreundlichkeit vs. Proportionalität		Vermeidung menschlicher Fehler im Straßenverkehr vs. Maschinen treffen ethische Entscheidungen		
Folgen-Abwägung	Interessen-Abwägung	Sicherheit vs. Privatsphäre		Vorhersage von Verbrechen vs. Analyse unschuldiger Personen	Beaufsichtigung von Kindern mittels Wearables/Toys vs. Verlust der Privatsphäre	Drohnen werden zur Überwachung eingesetzt vs. Eingriff in die Privatsphäre
Folgen-Abwägung	Interessen-Abwägung	Kundennutzen vs. Privatsphäre	Apps schlagen auf Basis des Standortes interessante Orte in der Nähe vor vs. Schutz der privaten Daten	Vorfilterung von Kommunikation und Informa-tionen auf Basis der Daten des Nutzers vs. Selbst-bestimmung des einzelnen		Unterstützung der menschlichen Pflegekräfte durch Roboter vs. „unpersönliche" Pflege
Folgen-Abwägung	Interessen-Abwägung	Kundenfreude vs. Willensfreiheit			Enge Interaktion via Sozialer Netzwerke u.ä. vs. Einsatz von Bots zur Beeinflussung der öffentlichen Meinung	
Folgen-Abwägung	Werte-Abwägung	Gruppenbedürfnisse vs. Einzelbedürfnisse		Optimierung des Verkehrsflusses reduziert Emissionen vs. Erstellung von Bewegungsprofilen		Entfall menschlicher Fehler durch Einsatz von Robotern vs. Wegfall von Jobs
Folgen-Abwägung		Kurzfristige Vorteile vs. Langfristige Risiken		Anpassung des Lernprogramms an Lernende vs. Sortierung von Menschen durch Maschinen	„Connected Everything" mit der Möglichkeit immer mit jedem zu kommunizieren vs. Fehlende soziale Interaktion	

Der Ansatz des „Praxisleitfaden zu den Algo.Rules" geht von einem ganzheitlichen Lebenszyklus datengestützter Anwendungen aus, der digitalethische Reflexionen als konstitutiven Bestandteil von Data-Governance begreift. Hier werden auf der Grundlage von neun, mit etwa 400 Beteiligten ausgearbeiteten Regeln detaillierte Checklisten mit Orientierungsfragen angeboten, mit deren Hilfe die digitalethischen Anforderungen bei der Gestaltung gesellschaftlich relevanter Datenverarbeitungssysteme abgeglichen und anwendungsspezifisch in einen Maßnahmenkatalog überführt werden können. Die zugrundeliegenden Regeln sind an dieser Stelle nur stichwortartig[14] aufgeführt:

1. Kompetenz aufbauen
2. Verantwortung definieren
3. Ziele und erwartete Wirkung dokumentieren
4. Sicherheit gewährleisten
5. Kennzeichnung durchführen
6. Nachvollziehbarkeit sicherstellen
7. Beherrschbarkeit absichern
8. Wirkung überprüfen
9. Beschwerden ermöglichen

Beide Ansätze beruhen auf unterschiedlichen Ausgangsszenarien und dienen an dieser Stelle nur als Beispiele, wie man den digitalethischen Reflexionsprozess systematisch gestalten könnte. Wie es die jeweiligen Institutionen in eigenen Geschäftsbereichen angehen oder sogar eigene Leitfäden entwickeln, steht selbstverständlich den Verantwortlichen frei. ▸

[14] Eine detaillierte Ausführung findet sich unter dem Link: https://irights-lab.de/praxisleitfaden/

5. Zusammenfassung

Zusammenfassend lässt sich feststellen, dass die Digitale Ethik als ein Reflexionsprozess verstanden werden soll, der organisationsübergreifend mit Einbeziehung unterschiedlicher Akteure zu gestalten ist. Es muss eine Verständigung über grundlegende ethische Prinzipien und Leitlinien stattfinden, um diese in bereichsspezifische Herausforderungen zu übersetzen. Als Grundlage für solche Grundprinzipien würde sich beispielsweise das verfassungsimmanente Menschenbild des Grundgesetzes besonders eignen. Ausgehend von ethischen Leitlinien sollen bestimmte Problemsituationen identifiziert, konkrete ethische Fragestellungen ausformuliert, unterschiedliche Perspektiven auf den spezifischen Problemfall beleuchtet und bestimmte Lösungswege ausgearbeitet werden. Die Rolle von Datenschutzbeauftragten kann dabei insbesondere darin bestehen, die am Diskurs beteiligten Akteure hinsichtlich rechtlicher Mindestanforderungen, des Status quo ihrer gegenwärtigen Umsetzung, der Interpretationsspielräume und gegebenenfalls der „weißen Flecken" der Rechtsregulierung im konkreten Anwendungsbereich sowie der technologischen Anforderungen zu beraten, damit sie ethisch vertretbare digitale Lösungen informiert und sachgerecht beurteilen können.

Über den Autor

Dr. Nikolai Horn
ist Projektkoordinator beim unabhängigen Think Tank iRights.Lab und ehrenamtlich Leiter der AG Ethik des parteipolitisch unabhängigen digitalpolitischen Netzwerkes Initiative D21. Nach seinem Studium der Philosophie arbeitete er am Institut für Öffentliches Recht der Universität Bonn (Lehrstuhl Prof. Dr. Dr. Udo Di Fabio) und promovierte mit einer interdisziplinären Arbeit zum Grundrecht der Gewissensfreiheit. Von 2015 bis 2017 war Horn Grundsatzreferent bei der Stiftung Datenschutz. Anschließend war er als Project Manager beim IT-Beratungshaus Capgemini mit Digitalisierungsansätzen im Öffentlichen Sektor sowie mit der Beratung von Bundes- und Landeseinrichtungen betraut.

▶ https://irights-lab.de/#lab

Anzeige

2BAdvice
PrIME ®

Bestellen Sie unsere KOSTENLOSE Einzelplatzversion

Datenschutzmanagement Plattform von Datenschutzexperten

Führende Datenschutz-Software bei mehr als 4000 Unternehmen im Einsatz

Neue Version 7.01

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

DATENSCHUTZ UND ETHIK: WIDERSPRUCH ODER HARMONIE?

Bernd Schütze

„Datenschutz ist Täterschutz" – ein Satz, den jeder Datenschutzbeauftragte so oder in ähnlicher Weise schon einmal vernahm. Der Satz ist genauso richtig oder falsch wie der Satz „Politiker töten Menschen". Natürlich beinhalten einige Entscheidungen von Politikern auch den Tod von Menschen, beispielsweise wenn sich gegen eine Geschwindigkeitsbeschränkung entschieden wird, medizinische Leistungen auf Grund von Zulassungsbeschränkungen oder Budget-Vorgaben der Krankenkassen nicht erbracht werden oder Soldaten in einen Einsatz in ein Kriegsgebiet geschickt werden. Gleichermaßen dient der Datenschutz dazu, alle Menschen vor dem Missbrauch ihrer Daten zu schützen, und dies schließt selbstverständlich „Täter" mit ein, wenn diese denn Menschen sind.

Die Wertung, ob eine Handlung „gut" oder „schlecht" ist, ist zunächst vom Rechtsrahmen losgelöst. Eine Handlung kann durch eine rechtliche Norm erlaubt sein, trotzdem wird sie als „falsch" gewertet. Steuerhinterziehung beispielsweise ist rechtlich verboten, laut einer Studie[1] erfolgt Steuerhinterziehung in Deutschland aber am zweithäufigsten in der EU. Ist Steuerhinterziehung daher gesellschaftlich anerkannt und akzeptiert? Ist Steuerhinterziehung also „gut" und nur rechtlich nicht erlaubt? Um diese und andere Fragen, insbesondere auch der Aussage „Datenschutz ist Täterschutz", beurteilen zu können, muss man sich mit ethischen Fragen beschäftigen. Aber was ist Ethik eigentlich?

Ethik: Eine (sehr) kurze Einführung

Ethik ist die philosophische Begründung von Moral und eine der ältesten Tätigkeitsbereiche in der Philosophie. Aristoteles philosophierte schon im alten Griechenland in seiner Nikomachischen Ethik über die Theorie des Guten, im Mittelalter leitete der Niederländer Baruch de Spinoza Ethik von der Ontologie Gottes ab und natürlich waren und sind ethische Themen auch in der Neuzeit immer wieder Ausgangspunkt für zahllose Debatten[2]; am kontroversesten wurden vielleicht die Thesen von Theodor W. Adorno zur Moralphilosophie diskutiert.

Aristoteles am Schreibpult (Quelle: artist unknown/public domain, Wikimedia Commons)

[1] Tax Research LLP: The European Tax - GapA report for the Socialists and Democrats Group in the European Parliament. [Online] 2020 [Zitiert 2020-06-02] Verfügbar unter http://www.taxresearch.org.uk/Documents/EUTaxGapJan19.pdf

[2] Natürlich sehr verkürzt; bei Ortmanns z. B. findet man eine immer noch kurze, aber deutlich ausführlichere Einführung über die Entwicklung der Ethik: Ortmanns W: Entwicklung der Ethik. In. Gestring/Gonschorek/Haubold/Sonntag/von der Weth (Hrsg.) Ethik im Mittelstand. Springer Verlag 2016. ISBN 978-3-658-09551-2

Ethik wird oftmals mit „Moral“ gleichgesetzt, wobei hierbei letztlich nur ein Ausdruck durch einen anderen ersetzt wird. Ethik ist eine kritische Auseinandersetzung mit aus der Gesellschaft resultierenden normativen Forderungen und Annahmen, denen gut und schlecht beziehungsweise richtig und falsch innewohnt; mitunter wird auch die Unterscheidung zwischen human und inhuman einbezogen.

Angewandte Ethik

Wenn sich Ethik mit von der Gesellschaft festgelegten normativen Ansprüchen, Regeln und Überzeugungen auseinandersetzt, handelt es sich um „angewandte“ Ethik. Angewandt im wissenschaftlichen/universitären Sinne der Philosophielehre bedeutet, dass die Aussage „angewandt worauf“ besprochen wird. Gesellschaftliche Wertvorstellungen ändern sich mit der Zeit. Wer in der Epoche der Französischen Revolution von der damaligen adligen Führungselite als „Terrorist“ bezeichnet wurde, gilt heute vielleicht in Geschichtsbüchern als Freiheitskämpfer.

Angewandte Ethik versucht, zu Ergebnissen zu kommen, wie „man“ sie interpretiert, wobei „man“ die aktuelle herrschende Interpretation der betrachteten Fragestellungen darstellen – je nach gesellschaftlichem Kontext. Eine ethische Festlegung, was als „gut“ und was als „falsch“ anzusehen ist, bildet also nicht „die“ Wahrheit ab, sondern die Wahrheit, wie man sie aktuell wahrnimmt. Noch im Mittelalter sollten Tiere und Menschen nicht leiden, weshalb sie bei Krankheit getötet wurden. Heute wird diskutiert, ob man einem todkranken Menschen erlauben darf, sich selbst zu töten oder ob man als Gesetzgeber die Selbstbestimmung von Menschen negieren kann – eine Frage, die das Bundesverfassungsgericht inzwischen zu Gunsten der Selbstbestimmung des Menschen entschied[3].

Um „Datenschutz“ (auch hier müsste man fragen: was ist das?) im Rahmen einer „angewandten Ethik“ zu betrachten, muss also der gesellschaftliche Kontext betrachtet werden.

Informationsethik

Im Bereich der Informationstechnik etablierte sich schnell die Erkenntnis, dass derart innovative Technik immer auch ethische Fragen beinhaltet. Schon 1994 verabschiedete die Gesellschaft für Informatik (GI) „Ethische Leitlinien“[4], 2018 wurde die dritte Version veröffentlicht[5]. Die Informationsethik untersucht die Moral sowohl von denjenigen, die Informations- und Kommunikationstechnologien und sogenannte „Neue Medien“[5] anbieten, als auch von denen, die diese Angebote nutzen. Die Informationsethik gehört zur angewandten Ethik und zu den Bereichs- oder Spezialethiken. Wer sich mit ethischen Fragen der automatisierten oder teilautomatisierten Verarbeitung von Daten beschäftigt, landet letztlich bei der Informationsethik. Dabei ist Informationsethik oftmals eine Querschnittsdisziplin, zum Beispiel wenn ethische Fragen bei Militärdrohnen betrachtet werden, ist immer auch die Militärethik mit dabei.

Gesellschaftliche Grundlage für ethische Betrachtungen

Die grundlegende Frage lautet[7]: Was sind die ethischen Maßstäbe, die einen Menschen durch seinen Beruf, sein Amt oder seine Rolle bei seiner Handlungsverantwortung leiten sollten? Die grundlegenden Maßstäbe finden sich in Deutschland in Artikel 1 und Artikel 2 des Grundgesetzes[8]:

Artikel 1:

1. Die **Würde** des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.
2. Das Deutsche Volk bekennt sich darum zu **unverletzlichen und unveräußerlichen Menschenrechten** als **Grundlage** jeder menschlichen Gemeinschaft, des **Friedens und der Gerechtigkeit in der Welt.**
3. Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2:

1. Jeder hat das Recht auf die **freie Entfaltung seiner Persönlichkeit**, soweit er **nicht die Rechte anderer verletzt** und **nicht gegen die verfassungsmäßige Ordnung** oder das **Sittengesetz verstößt**.
2. **Jeder** hat das **Recht auf Leben und körperliche Unversehrtheit.** Die **Freiheit der Person ist unverletzlich.** In diese Rechte darf nur aufgrund eines Gesetzes eingegriffen werden.

Wie man auf den ersten Blick sieht, ist das Grundgesetz nicht nur auf deutsche Bürger ausgelegt.

[3] BVerfG, Urt. v. 2020-02-26, AZ 2 BvR 2347/15. [Online] 2020 [Zitiert 2020-06-02] Verfügbar unter https://www.bundesverfassungsgericht.de/e/rs20200226_2bvr234715.html

[4] Rödiger KH, Wilhelm R. (1996) Zu den Ethischen Leitlinien der Gesellschaft für Informatik. Informatik-Spektrum (19):79–86

[5] Gesellschaft für Informatik (GI): Ethische Leitlinien. [Online] 2020 [Zitiert 2020-06-10] Verfügbar unter https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien

[6] Zum Begriff „Neue Medien“ siehe auch Wikipedia: Neue Medien. [Online] 2020 [Zitiert 2020-06-10] Verfügbar unter https://de.wikipedia.org/wiki/Neue_Medien

[7] Angelehnt an: Walter Schweidler: Kleine Einführung in die Angewandte Ethik. Kap. 2.1 „Der ethische Gesichtspunkt“. Springer Verlag, 2018. ISBN 978-3-658-14031-1, https://doi.org/10.1007/978-3-658-14032-8

[8] Richter T: Gesetze als Grundlage ethischen Handelns. In. Gestring/Gonschorek/Haubold/Sonntag/von der Weth (Hrsg.) Ethik im Mittelstand. Springer Verlag 2016. ISBN 978-3-658-09551-2

Vielmehr gelten die ethischen Maßstäbe des Grundgesetzes für alle Menschen, die in Deutschland oder anderswo mit deutschen Staatsorganen in Berührung kommen, eine Tatsache, welche dem Bundesnachrichtendienst erst durch das Bundesverfassungsgericht verdeutlicht werden musste[9].

Die Würde des Menschen (oft kurz Menschenwürde genannt) ist zunächst einmal ein Wert, der allen Menschen gleichermaßen und unabhängig von ihren Unterscheidungsmerkmalen wie Herkunft, Geschlecht, Alter oder Status zugeschrieben wird. Auch das, was unter dem Begriff „Menschenwürde" zu verstehen ist, änderte sich im Verlauf der Geschichte. Schon Cicero nutze das gesellschaftliche Konzept „dignitas" in seinen Werken wie „De re publica" oder „De officiis". Cicero bezog Würde jedoch immer auf die persönliche Leistung eines Einzelnen für sein Gemeinwesen; heute wird Menschenwürde anders interpretiert. Die Menschenwürdegarantien im Grundgesetz gewährleisten, dass die Menschenwürde keiner Abwägung und keiner Bilanzierung mit anderen Gütern und Rechten unterliegen soll.

In der Rechtsphilosophie ist die Menschenwürde heute als rechtlicher Leitbegriff für ein humanistisch bestimmtes Staats- und Gesellschaftsverständnis anzusehen[10]. Nach der Rechtsprechung des deutschen Bundesverfassungsgerichts ist jede Einschränkung der Menschenwürde rechtswidrig, ohne dass eine Rechtfertigung möglich wäre[5]. Dabei ist es egal, ob der Mensch Täter oder Opfer, ehrenwerter Bürger oder Straftäter ist – die Menschenwürde ist allen Menschen zu eigen.

„Datenschutz ist Täterschutz" – eine ethische Bewertung der Aussage

Wie in Abschnitt „Gesellschaftliche Grundlage für ethische Betrachtungen" dargestellt wurde, gilt die Menschenwürde für alle Menschen gleichermaßen. Aufgabe des Datenschutzrechts ist es die informationelle Selbstbestimmung[11] als Ausprägung des aus Artikel 2 Absatz 1 Grundgesetz in Verbindung mit Artikel 1 Absatz 1 Grundgesetz abgeleiteten allgemeinen Persönlichkeitsrechts zu schützen. Somit muss das Datenschutzrecht alle Menschen schützen, und damit natürlich auch Täter.

Da das Grundgesetz die Grundlage für die ethische Betrachtung darstellt, sind entsprechende Äußerungen nicht unethisch, wenn die Aussage im feststellenden Sinne getroffen wird. Als Aufforderung, dass Datenschutz für Täter nicht gelten darf, ist die Aussage als im höchsten Maße unethisch anzusehen: Wer diese Tatsache als Anklage versteht, will letztlich, dass die Menschenwürde entgegen Artikel 1 Grundgesetz nicht für alle Menschen gilt, letztlich stellen sich Menschen mit dieser Forderung gegen das Grundgesetz, insbesondere bei Beamten oder Mitgliedern der Bundesregierung kann dies einen Verstoß gegen ihren Amtseid[12] bedeuten.

Ethik und Technik

Der Einsatz neuer Techniken ist inzwischen fest mit dem Alltag etabliert, Informationstechnik ist aus dem täglichen Leben nicht mehr wegzudenken: sei es bei der Steuerung von Ampelanlagen, bei Kurs- und Kollisionsberechnungen für Flugzeuge oder Schiffe oder bei bewaffneten Kampfdrohnen – überall begegnet man direkt oder indirekt der Nutzung von Informationstechnologien. Dabei wirkt die jeweilige nationale Kultur auf die Phasen der Gestaltung von Informationssystemen ein[13], sodass immer auch bei der ethischen Betrachtung dieser Techniken der jeweilige gesellschaftliche Kontext betrachtet werden muss.

Ist etwas derart tief in das Leben der Menschen integriert, gibt es aber ethische Grundsätze, die in diesem Umfeld immer berücksichtigt werden müssen[14]:

- Die für den Menschen nutzbaren Ressourcen sind begrenzt, daher ist eine technische Neuerung ethisch nur gerechtfertigt, wenn der bisherige Nutzen mit einem geringerem Aufwand als bisher erreicht wird.
- Menschen streben nach einer stetigen Lebensverbesserung, einem höheren Wohlstand. Eine Grenze dieses Strebens besteht in der gesamtgesellschaftlichen Akzeptanz technischer Neuerungen. Eine Steigerung individueller Lebensverbesserungen zulasten der Bevölkerung ist aus ethischer Sicht abzulehnen.
- Da der Lebensraum der Menschen auf die Erde beschränkt ist sind Auswirkungen technischer Neuerungen auf die Lebensräume zu bedenken.
- Technische Neuerungen müssen eine Minimierung sowohl von Gefährdungen des Lebens als auch der Gesundheit von Menschen beinhalten. Dies schließt allein schon aus den vorhergehenden Erwägungen soziale und umweltbezogene Ressourcennutzung ein. ▶

[9] BVerfG, Urt. v. 2020-05-19, AZ 1 BvR 2835/17. [Online] 2020 [Zitiert 2020-06-02] Verfügbar unter https://www.bundesverfassungsgericht.de/e/rs20200519_1bvr283517.html

[10] Hilgendorf E: Menschenrechte, Menschenwürde, Menschenbild. In: Hilgendorf E, Joerden JC (Hrsg.), Handbuch Rechtsphilosophie. Springer Verlag, 2017. ISBN 978-3-476-02433-6, https://doi.org/10.1007/978-3-476-05309-1_51

[11] BVerfG, Urt. v. 1983-12-15, AZ 1 BvR 209/83. [Online] 2020 [Zitiert 2020-06-02] Verfügbar unter https://www.bundesverfassungsgericht.de/e/rs19831215_1bvr020983.html

[12] Wikipedia: Eidesformel. [Online] 2020 [Zitiert 2020-06-02] Verfügbar unter https://de.wikipedia.org/wiki/Eidesformel#Bundespr%C3%A4sident,_Mitglieder_der_Bundesregierung

[13] Kummer TF, Leimeister JM, Bick M. (2012) Die Bedeutung von nationaler Kultur für die Gestaltung von Informationssystemen. Wirtschaftsinformatik (54): 303–318

[14] Angelehnt an: Schweidler W.: Kleine Einführung in die Angewandte Ethik. Kap. 4.1.2.2 „Ethische Kriterien für die Technik". Springer Verlag, 2018. ISBN 978-3-658-14031-1, https://doi.org/10.1007/978-3-658-14032-8

Wenn Daten als das „neue Öl" bezeichnet werden,[15] welches für die Datenwirtschaft fließen muss, so sind selbstverständlich (nicht nur) die obigen Aspekte zu betrachten: Wenn der Gesetzgeber die informationelle Selbstbestimmung der Menschen beschränken will, damit andere die personenbezogenen Daten zu ihrem wirtschaftlichen Vorteil nutzen können, so ist zu fragen: Was nützt es der Bevölkerung im Ganzen? Und hier sind konkrete, überprüfbare Antworten zu fordern; allgemeine Aussagen wie „schafft Arbeitsplätze" werden zumindest im Rahmen einer ethischen Bewertung in dieser Allgemeinheit dazu führen, dass die Entmündigung der Bürger als unethisch anzusehen ist. Datenschutz ist in diesen Fällen als Schutz des Persönlichkeitsrechts vor Missbrauch der personenbezogenen Daten anzusehen.

Allerdings kann auch das Datenschutzrecht unethische Aspekte annehmen. Das Datenschutzrecht verbietet allgemeine Einwilligungen in eine Verarbeitung personenbezogener Daten. Es ist einem Bürger nicht möglich, beispielsweise einem Mediziner die Erlaubnis der Nutzung all seiner Daten zu medizinischer Forschung zu geben – der Verarbeitungszweck ist entsprechend den datenschutzrechtlichen Vorgaben zu unkonkret. Betroffene Personen besitzen das Recht auf „Nicht-Wissen", dieses Recht resultiert auch als „negative" Form des „Rechts auf informationelle Selbstbestimmung".[16] Wie kann dieses Recht durch den „Zwang zur Aufklärung" bei Einholung einer Einwilligung aufgehoben werden, wenn hierbei nicht zugleich die informationelle Selbstbestimmung der betroffenen Personen eingeschränkt wird?

Wie jeglicher Schutz kann auch der Datenschutz zu einer eigentlich nicht gewollten Beschränkung führen. Wenngleich das Datenschutzrecht geschaffen wurde, um betroffene Personen bei einem Ungleichgewicht der Kräfte vor einem Missbrauch der eigenen Daten zu schützen, kann das Datenschutzrecht gleichermaßen eine unethische Entscheidung erzwingen und betroffenen Personen im Einzelfall das Recht auf informationelle Selbstbestimmung verweigern.

Datenschutz, Ethik und neue Technologien

Jede neue Technik wirf immer auch ethische Fragen auf. Am Beispiel der Cloud-Nutzung und der künstlichen Intelligenz wird einführend dargestellt, wie man sich derartigen Fragestellungen nähern kann.

Cloud

Immer mehr Unternehmen transferieren Daten ihrer Kunden in die Cloud. Dabei stellt sich die Frage, ob dem einstellenden Unternehmen alle Konsequenzen des Vorgangs bewusst sind. Beispielsweise könnte man fragen:

- Was ist etwa, wenn Inhalte seitens des Cloud-Dienstleisters als Auftragsverarbeiter als verdächtig angesehen werden und dieser die betreffenden Informationen an Behörden weiterleiten?
- Was ist, wenn lebenswichtige Daten aufgrund eines Vorfalls oder Vorkommnisses beim Dienstleister öffentlich bekannt oder vernichtet werden?
- Wie stark ist die Abhängigkeit und wie weit geht der Kontrollverlust, die mit der Übergabe der personenbezogenen Daten in die Gewalt eines Dienstleisters immer verbunden sind?

Letztlich sind es ähnliche Fragen, die sich auch bei der Verarbeitung ohne den Cloud-Dienst stellen. Der Cloud-Dienst bedingt durch die Einschaltung eines Dienstleisters und einer aufgrund des Cloud-Einsatzes vorhandenen Erreichbarkeit der Daten über das Internet zusätzliche Gefahren, die eingegangen werden, weil sich der Verantwortliche einen wie auch immer gearteten Vorteil davon verspricht. Letztlich werden also personenbezogene Daten eines Kunden einer Gefahr ausgesetzt, um einen eigenen Vorteil zu erlangen. Rechtlich kann dies erlaubt sein, wenn entsprechende Verträge etwa zur Auftragsverarbeitung geschlossen werden. Ethisch müssen – wie immer – die Rahmenbedingungen betrachtet werden. Wurden die Kunden vor Erhebung der Daten über die Verarbeitung in der Cloud informiert und gaben sie die Daten mit diesem Wissen freiwillig dem Verantwortlichen, wird dies ethisch anders zu bewerten sein, als wenn der Verantwortliche ohne Zustimmung der Kunden – eventuell auch nachträglich durch späteres Outsourcing der Verarbeitung - beschloss, für die Verarbeitung der personenbezogenen Kundendaten eine Cloud zu nutzen.

Künstliche Intelligenz

Man unterscheidet zwischen „schwacher" und „starker" KI[17]: Schwache KI simuliert Intelligenz, starke KI ist intelligent. Beispiele für schwache KI sind Umsetzungen konkreter Fragestellungen wie beispielsweise Schach spielen oder auch Musik kom-

[15] Axel Springer SE – Welt: Und dann entdeckt Merkel das „neue Öl". [Online] 2019 [Zitiert 2020-06-02] Verfügbar unter https://www.welt.de/politik/deutschland/article203620526/Digitalstrategie-der-Regierung-Und-dann-entdeckt-Merkel-das-neue-Oel.html

[16] BGH sieht zur Anwendung dieses Rechts auch Voraussetzungen. Siehe BGH, Urt. v. 2014-05-20, AZ VI ZR 381/13. Rn. 14, 15 [Online] 2014 [Zitiert 2020-06-02] Verfügbar unter http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=67940&pos=0&anz=1

ponieren. Merkmal einer starken KI ist, dass diese künstliche Intelligenz der des Menschen gleicht oder diese sogar übertrifft. Bis heute existiert keine „starke" KI.

Bisherige KI-Anwendungen bestehen aus IT-Lösungen und Methoden, welche selbstständig Aufgaben erledigen, wobei die der Verarbeitung zugrunde liegenden Regeln nicht zwingend durch den Menschen vorgegeben sein müssen[18]. Beispiele für heute existierende KI-Anwendungen sind Übersetzungsdienste (z. B. https://www.deepl.com/translator) oder die in Suchmaschinen eingesetzten Korrekturvorschläge (z. B. https://www.google.de).

Der Branchenverband bitkom veröffentlichte ein „Periodensystem der KI", welches eine systematische Übersicht über verschiedene Anwendungsszenarien für KI bietet, ohne dass man sich in den Tiefen der dahinterliegenden Technik verliert[19].

Die „schwache" KI beinhaltet diverse Risiken. Zum einen besteht immer die Gefahr einer Diskriminierung[20]. Denn KI benötigt Daten des wirklichen Lebens, aufgrund derer ein „Lernprozess" entsprechend den von den Software-Entwicklern definierten Regeln erfolgt. Diese Voraussetzungen beinhalten jedoch zwei Folgen:

1. Menschen legen die Regeln fest, mit denen eine KI Daten verarbeitet. Werden von den Entwicklern eigene Annahmen, „anerkannte Tatsachen" oder Ähnliches in diese Regeln integriert, so wird die KI zwangsläufig mit diesen Vorgaben arbeiten müssen – was zu Diskriminierungen führen kann.
2. Beinhalten die Daten der wirklichen Welt bereits eine Diskriminierung (z.B. Vorstände in DAX-Unternehmen sind männlich), so wird auch diese im täglichen Leben angewandte Diskriminierung von der KI „gelernt".

Weiterhin können Trainingsdaten Fehler enthalten. Ist dies der Fall, so werden auch die mit der KI erzeugten Resultate Fehler enthalten (müssen). Fehler in Trainingsdaten sind in der Regel unabsichtlich enthalten, beispielsweise weil im Sinne von Big Data einfach eine unkontrollierte Datensammlung als Trainingsdaten genutzt wurde oder weil bei der – eigentlich sorgfältig durchgeführten - Auswahl der Trainingsdaten Fehler nicht entdeckt wurden.

Sowohl fehlerhafte Trainingsdaten als auch eine vorhandene Diskriminierung bei KI-gestützten Entscheidungen führen – denkt man an die im Abschnitt „Ethik und Technik" angesprochenen Grundsätze – zu dem Ergebnis, dass der Einsatz von künstlicher Intelligenz aus ethischer Sicht Bedenken hervorruft.

Bedenkt man zudem, dass bei Nutzung von KI oftmals von einer „Blackbox" gesprochen wird, weil Menschen nicht nachvollziehen können, wie die Maschine mittels KI zu einer Entscheidung kam, so resultiert der Einsatz von KI mit den oben genannten Prämissen faktisch immer zu einer Einschränkung des Rechts auf informationelle Selbstbestimmung bei den Personen, um die es bei diesen Entscheidungen geht.[21]

Datenschutzrecht vs. Recht auf informationelle Selbstbestimmung

Wenngleich das Recht auf informationelle Selbstbestimmung als eine Form des aus der Achtung der Menschenwürde resultierenden allgemeinen Persönlichkeitsrechts anzusehen ist, gilt dies nicht notwendigerweise für das Datenschutzrecht. Wenn Verantwortliche, Datenschutzbeauftragte oder auch Datenschutz-Aufsichtsbehörden das Datenschutzrecht anwenden und für die betroffene Person entscheiden, was mit den Daten geschehen darf und was nicht, so wird letztlich die betroffene Person ihrer Rechte beraubt. Entsprechend Artikel 2 Absatz 2 Grundgesetz ist dies erlaubt, denn die Gesetze beinhalten diese Möglichkeit. Aus ethischer Sicht muss man dies aber differenzierter betrachten.

Da gerade unter der Covid-19-Pandemie vielfältige Diskussionen zur Verwendung personenbezogener Daten erfolgen, erscheint die Nutzung medizinischer Daten ein gutes Beispiel für die Betrachtung der Sekundärnutzung dieser Daten aus ethischer Sicht zu sein. Folgendes Szenario:

- Personenbezogene Daten wurden im Rahmen der Patientenbehandlung in einem Krankenhaus erhoben. Ausschließlicher Zweck der Datenverarbeitung war die Behandlung der betroffenen Person. Jetzt sollen die Daten für Forschungszwecke verarbeitet werden. Tabelle 1 zeigt beispielhaft verschiedene Szenarien in der medizinischen Forschung.

Rechtlich kann eine mehr oder weniger eindeutige Bewertung durch Datenschutzbeauftragte oder Datenschutz-Aufsichtsbehörden unter Nutzung der jeweiligen Gesetze erfolgen. ▶

[17] Universität Oldenburg: Schwache KI und Starke KI. (2008/2009). Online, zitiert am 2020-06-09; Verfügbar unter http://www.informatik.uni-oldenburg.de/~iug08/ki/Grundlagen_Starke_KI_vs._Schwache_KI.html

[18] Claudia Dukino: „Was ist Künstliche Intelligenz? Eine Definition jenseits von Mythen und Moden". Fraunhofer Blog, 2019-03-14. Online, zitiert am 2020-09-09; Verfügbar unter https://blog.iao.fraunhofer.de/was-ist-kuenstliche-intelligenz-eine-definition-jenseits-von-mythen-und-moden

[19] bitkom: KI Periodensystem. Online, zitiert am 2019-08-03; Verfügbar unter https://periodensystem-ki.de/

[20] Aktuelles Beispiel: Forscher veröffentlichten, dass KI auch bei 175 Milliarden Parametern Frauen und Männern Stereotype zuordnet. Artikel: Brown et al. (2020) Language Models are Few-Shot Learners. Online, zitiert am 2020-09-09; Verfügbar unter https://arxiv.org/pdf/2005.14165.pdf

[21] Mehr zum Thema KI und Ethik z. B. unter Jobin A., Ienca M., Vayena E. (2019) The global landscape of AI ethics guidelines. Nature Machine Intelligence (1): 389-399

Forschungszweck	Forschende	Datenschutzrecht
Forschung im Umfeld der behandelnden Abteilung	Behandelnde Personen im Krankenhaus	Erlaubt durch Landeskrankenhausgesetz (LKG)
Gemeinsame Forschung mehrerer Behandlungseinrichtungen	Personen, die nicht in die Behandlung involviert waren	Einzelne LKG erlauben dies, andere verlangen Interessensabwägung, andere LKG nur mit Einwilligung
Aufgrund einer aktuellen Pandemie sollen Daten Dritten zu Forschungszwecken zur Verfügung gestellt werden	Dritte	Nur mit Einwilligung der betroffenen Personen
Zusammenführung der Daten mit Sozialdaten zu Forschungszwecken, die nicht in § 75 Absatz 1 SGB X genannt wurden	Behandelnde Personen im Krankenhaus	Auch mit Einwilligung nicht erlaubt

Tabelle 1: Mögliche Szenarien in der medizinische Forschung

Bei einer ethischen Bewertung müssen hingegen andere Randbedingungen einbezogen werden:

1. Eine nachträgliche Einwilligung einzuholen ist eher theoretisch möglich. Studien ergaben, dass Rücklaufquoten bei begleitenden telefonischen Nachfragen zur Anfrage bis zu 12 Prozent erreichen, ohne Nachfragen (die datenschutzrechtlich ja auch schon einen Erlaubnistatbestand benötigen) ist eine Rücklaufquote von acht Prozent schon ein sehr gutes Ergebnis. In den Studien wurde nachgefragt, ob die Menschen, die keine Rückmeldung abgaben, etwas gegen die Nutzung haben: Den meisten war es egal, einige waren sogar dafür, nur sehr wenige waren dagegen. Aber der Aufwand, die schriftliche Einwilligung (die in vielen Bereichen der medizinischen Forschung immer noch vorgeschrieben ist) an die anfragenden Forscher zurückzusenden, war ihnen einfach zu groß. Bei einer ethischen Betrachtung muss neben dem Nutzen der Forschung für die Menschen daher auch berücksichtigt werden, dass ein Großteil der Betroffenen nichts gegen eine Nutzung ihrer Daten für diese Zwecke haben, einige wenige hingegen schon.

2. Der Zweck der Forschung muss natürlich betrachtet werden. Handelt es sich um eine Promotion oder Habilitation, die eher der forschenden Person als der Gesellschaft im Ganzen nutzt, da die Forschungsergebnisse für die Behandlung der Menschen keinen oder nur wenig Nutzen bringt? Handelt es sich um die Bekämpfung einer Erkrankung wie ein Krebsleiden, woran die Gesellschaft ein starkes Interesse hat? Oder soll gar eine Pandemie bekämpft werden, welche die Menschheit bedroht? Artikel 2 Absatz 2 Grundgesetz enthält den Passus „soweit er nicht die Rechte anderer verletzt", die körperliche Unversehrtheit beziehungsweise die Erlangung eines Heilmittels gegen Erkrankungen ist gegenüber dem Recht auf die freie Entfaltung seiner Persönlichkeit also abzuwägen.

3. Gerade medizinische Daten beinhalten oftmals nicht nur Daten einer Person. Genetische Daten beinhalten grundsätzlich auch Informationen von Verwandten, insbesondere von Eltern, Großeltern, Geschwistern und Kindern. Auch bei erblichen Erkrankungen sind regelhaft auch andere Personen von einer Datennutzung betroffen. Auch deren Recht auf informationelle Selbstbestimmung ist zu beachten. Betrachtet man es als unethisch, wenn Datenschutzbeauftragte oder Datenschutz-Aufsichtsbehörden einer betroffenen Person die Freigabe ihrer Daten zur Verarbeitung verbieten will, wenn aus Sicht des Datenschutzes aufgrund des Wunsches der betroffenen Person keine Aufklärung erfolgte, so ist dann auch die Fremdbestimmung zur Datennutzung von Verwandten durch die Entscheidung einer betroffenen Person als unethisch einzustufen.

4. Wie sind die Rahmenbedingungen bei der betroffenen Person selbst? An Demenz erkrankte oder auch Personen mit psychischen Erkrankungen können gegebenenfalls keine Entscheidung für sich selbst treffen. Rechtlich kann unter Umständen ein Betreuer entscheiden, aus ethischer Sicht ist aber fraglich, ob ein Betreuer die betreute Person so gut kennt, dass er tatsächlich so entscheidet, wie es die Person ohne ihre Erkrankung tun würde.

5. Gerade bei Erkrankungen, die einen großen Teil der Bevölkerung betreffen, kann der kollektive gesellschaftliche Wunsch nach einer Heilmöglichkeit dazu führen, dass die Rechte einzelner Individuen eingeschränkt werden. Aber dürfen Daten von in psychiatrischen Kliniken zwangseingewiesenen Menschen genutzt werden? Dürfen Daten von Straftätern in Gefängnissen genutzt werden? Ein nicht in

seiner Freiheit eingeschränkter Mensch kann – wenn ihm die Regelungen in einem Land völlig missfallen – auswandern und sich in einem anderen Land ansiedeln. Eingesperrte Menschen können sich der erzwungenen Verarbeitung ihrer Daten nicht entziehen. Allein schon aus diesen Aspekten können Einflüsse erwachsen, welche in eine ethische Betrachtung einfließen sollten. Aber natürlich sind auch viele andere ethische Fragestellungen in diesem Zusammenhang direkt offensichtlich, etwa inwieweit ein Gemeinnutzen überhaupt die erzwungene Mitarbeit einer eingesperrter Personen ethisch legitimieren kann.

Im Rahmen der konsequenzialistischen Ethik[22], welche den Zweck einer Handlung betrachtet, aber auch der deontologischen Ethik, deren Beurteilung sich eher an der inneren Einstellung des Handelnden orientiert, kann man unter Abwägung der moralischen Grundsätze der Gesellschaft gegebenenfalls zu anderen Ergebnissen als bei einer rechtlichen Betrachtung kommen. Um beim medizinischen Beispiel zu bleiben: Gerade ethische Betrachtungen erfordern eine Einbeziehung auch der Begleitumstände; gerade im medizinischen Kontext können die Begleitumstände – beispielsweise die Betrachtung der indirekt einbezogenen Personen bei Nutzung der Daten einer betroffenen Person – deutlichen Einfluss auf die Wertung enthalten. Die „Fremdbestimmung" betroffener Personen durch die das Datenschutzrecht ausübende Verantwortliche, durch Datenschutzbeauftragte oder auch durch die Datenschutz-Aufsichtsbehörden können aus ethischer Sicht je nach Begleitumständen „gut" oder „schlecht" sein: Erfolgt eine Verweigerung der Datennutzung und werden durch die Verweigerung Dritte wie Geschwister oder Kinder vor einer Fremdbestimmung geschützt, so wird man diese Verweigerung wahrscheinlich anders beurteilen, als wenn durch die Datenverarbeitung Dritte nicht involviert sind und die Verweigerung der Nutzung Daten des Betroffenen allein zu einer Fremdbestimmung und einem Entzug des Rechts auf informationelle Selbstbestimmung bedeutet.

Fazit

Datenschutz als Ausprägung des Rechts auf informationelle Selbstbestimmung ist letztlich ein Faktor, welcher die Menschenwürde gewährleistet. Das Datenschutzrecht selbst soll betroffenen Personen die Ausübung des Rechts auf informationelle Selbstbestimmung ermöglichen, beschränkt jedoch in einigen Regelungen selbst die informationelle Selbstbestimmung der betroffenen Personen, zum Beispiel durch die Vorgaben für eine rechtsgültige Einwilligung: Die betroffene Person muss für eine Einwilligung „aufgeklärt" sein, ob sie es will oder nicht.

Das von Datenschutzbeauftragten und den Datenschutz-Aufsichtsbehörden für die jeweils betroffene Person ausgeübte Datenschutzrecht muss man als Einschränkung des Rechts auf informationelle Selbstbestimmung werten, da hier Entscheidungen für statt durch die jeweils betroffene Person getroffen werden. Ob die getroffenen Entscheidungen als „ethisch" oder auch als „unethisch" zu bewerten sind, hängt – wie nahezu alles im Recht – vom konkreten Einzelfall ab.

Grundsätzlich ist es aber auch aus ethischer Sicht möglich und wünschenswert, wenn einzelne Personen in Bezug auf ihr Recht zum selbstbestimmten Leben zum Wohle der Gemeinschaft gut begründeten, klar definierten und – sofern möglich – zeitlich begrenzten Einschränkungen unterzogen werden. Im Rahmen der Covid-19-Pandemie wird viel über das Tracking von Personen geschrieben. Dieses Tracking muss neben (datenschutz-) rechtlichen auch ethischen Anforderungen genügen[23], dann kann ein Tracking nicht nur datenschutzrechtlich erlaubt, sondern ethisch auch geboten sein.

Über den Autor

Dr. Bernd Schütze

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

[22] zellux.net: Verschiedene Ethikansätze. [Online] 2020 [Zitiert 2020-06-02] Verfügbar unter https://zellux.net/m.php?sid=21, bzw. Konsequenzialistische Ethiken (https://zellux.net/m.php?sid=66), Deontologische Ethiken (https://zellux.net/m.php?sid=65)

[23] Siehe Morley J, Cowls J, Taddeo M, Floridi L. (2020) Ethical guidelines for COVID-19 tracing apps. Nature (582): 29-31

DIGITALE ETHIK UND ETHICS BY DESIGN

Prof. Dr. Petra Grimm

Die Digitale Ethik ist keine Kür, sie ist ein unverzichtbarer Wegweiser in einer komplexer und konfliktreicher gewordenen Gesellschaft. So stellen sich in vielen alltäglichen Lebenskontexten ethische Fragen, die normativer und werteorientierter Antworten bedürfen. Wenn es um die Akzeptanz ethisch normativer Standards geht, ist die Ethik im Unterschied zum Recht auf intrinsische Einsichten der Menschen und Konsens angewiesen. Erich Fromm hat dies in Bezug auf den Wert der „Verantwortung" eindrücklich formuliert: „Verantwortungsgefühl ist keine Pflicht, die dem Menschen von außen aufgezwungen wird, sondern die Antwort auf etwas, von dem man fühlt, dass es einen angeht. Verantwortung und Antwort haben die gleiche Wurzel: Verantwortlich sein heißt, zum Antworten bereit sein." (Fromm 2018: 115)

Ethical turn – der Ruf nach der Ethik?

Von Unternehmen wird zunehmend erwartet, sich in ethischen Fragen zu positionieren. Hintergrund hierfür ist ein im Zuge der Digitalisierung sich abzeichnender „ethical turn". Dieser Trend drückt sich in einem erhöhten Bedarf nach ethischer Orientierung, Einordnung und Bewertung aus. Nicht nur in der Bildung und Forschung, auch in Unternehmen wird der Ruf nach ethischer Expertise lauter. Dabei kann die Ethik im besten Fall als Steuerungsinstrument und Moderator fungieren, im schlechtesten Fall kann sie aber auch zur Abwendung drohender rechtlicher Maßnahmen missbraucht werden, was als „Ethics Washing" bezeichnet wird (Wagner 2018). Unbenommen aber ist, dass sich der ethical turn durch einen Wandel der Narrative abzeichnet. Narrative (was erzählt wird) und Narrationen (wie etwas erzählt wird) beeinflussen unsere Sicht auf die Welt und schreiben Phänomenen und Entwicklungen bestimmte Bedeutungen zu (Grimm/Müller 2016). Ebenso artikulieren sich Zeitgeist und gesellschaftliche Trends in entsprechenden Narrativen. Das ehemals populäre Narrativ „Ethik ist innovationshemmend", das Milton Friedmans bekanntes Diktum „The Social Responsibility of Business is to Increase its Profits" (1970) indirekt auf den Punkt brachte, wurde seit Ende

des letzten Jahrtausends zunehmend in Frage gestellt. Mit aufkommender Kritik an einer monopolistischen Digitalökonomie gewinnt ein neues Narrativ an Fahrt: „Ethische Standards sind wichtig." Das belegt auch die aktuelle BVDW-Studie (2019): Demnach würden 55 Prozent der Unternehmen die Auffassung vertreten, dass das Thema „Ethik" bei der Entwicklung neuer Produkte einen hohen oder sehr hohen Stellenwert habe. 74 Prozent der Verbraucher seien der Meinung, dass ethische Grundsätze bei der Entwicklung neuer Produkte eingehalten werden sollten. Zudem zeigt die Studie, dass in Deutschland ethische Standards zunehmend auch als Wettbewerbsfaktor und USP relevant werden: 72 Prozent der Bundesbürger würden solche Produkte oder Services bevorzugen, die so geplant sind, dass sie sich bei ihrer Entscheidungsfindung an nachvollziehbaren ethischen Standards orientieren. Im Gegenzug geben 71 Prozent der Digitalunternehmen an, dass diese Produkte auch potenziell erfolgreicher im Markt seien.

Topografie der Digitalen Ethik – um welche Werte geht es?

Ethik ist eine wissenschaftliche Disziplin, sie ist sowohl eine Theorie des richtigen Handelns als auch Reflexionstheorie der Moral. Die Ethik kann nicht nur Orientierung in moralischen Fragen liefern. Das heißt, es wird nicht nur reflektiert, wie der Einzelne gut handeln kann und was die Auswirkungen des Handelns auf die Anderen sind, sondern sie stellt auch die Frage, wie ein gutes Leben aussehen kann, und zwar für eine größtmögliche Anzahl von Menschen. Die Digitale Ethik befasst sich mit den Auswirkungen der Digitalisierung auf den Einzelnen und die Gesellschaft und leitet normative Standards daraus ab, die wiederum neue Anreize und Impulse setzen können, um ethische Prinzipien als Leitmotiv in zukünftige Handlungen einfließen zu lassen (Grimm/Keber/Zöllner 2019).

Zentrale Fragen sind: Wie sollen/wollen wir in einer digitalisierten Welt leben? Wie soll der Mensch handeln? Welche Werte bestimmen unser Leben? Ethik fragt nicht „Was ist technisch möglich?", sondern „Was ist wünschenswert?" und „Für wen ist das wünschenswert?"

Die Digitale Ethik als Erweiterung und Fortschreibung der Medienethik ist eine Angewandte Ethik. In einer Topografie beziehungsweise in einer Lagebeschreibung der Digitalen Ethik (vgl. Abb. 2) lassen sich sowohl die Werte, die in ethischen Diskursen und Leitlinien aktuell zur Diskussion stehen,[1] als auch die Risiken, die sich im Zuge der digitalen Entwicklung ergeben, beschreiben. Demnach stehen folgende Werte im Mittelpunkt: Menschenwürde, Autonomie des Einzelnen, Privatheit (auch als Voraussetzung für Autonomie), Wertschätzung der Stakeholder im Umgang miteinander, Vertrauen, das nicht zuletzt durch Kontrollierbarkeit, Erklärbarkeit und Transparenz automatisierter und autonomer Systeme entsteht, Gerechtigkeit und Verantwortung sowie die Anforderung an digitale Technik und deren Anwendung, demokratieverträglich zu sein. Als Risiken, die mit der Entwicklung, Gestaltung sowie ökonomischen und gegebenenfalls politischen Zielsetzung digitaler Technologien verbunden sind, lassen sich folgende identifizieren: Manipulation im Informationsbereich (Stichwort „Desinformation"), Machtasymmetrie von Nutzern und Anbietern (Stichworte „intransparente Datenverwertung" und „Abhängigkeit der Nutzer*innen von Intermediären") und Heteronomie (fehlende Selbstbestimmung, wenn automatisierte Systeme beispielsweise über Kreditvergabe, Prämien oder Jobs entscheiden). Überwachung von staatlicher Seite und durch Wirtschaftsunternehmen ist ein weiterer Risiko-Topos. Neben diesen systembezogenen Risiken, die ökonomisch und politisch begründet sind und regulierbar wären, haben wir es auch mit primär technologiebezogenen Risiken zu tun, die die Notwendigkeit einer Technikfolgenabschätzung, Ethics by Design und einer nachhaltigen Digitalökologie verdeutlichen. Zu letzteren Risiken gehören neben den Problemen des Dual-Use (das heißt der unintendierten Folgen) und der Biases (im Sinne von Verzerrungen, die zu Diskriminierung führen können) das noch in der Öffentlichkeit viel zu wenig beachtete Thema „klimaschädlicher Digitalsektor". Es ist zwar weitgehend bekannt, dass der Energiebedarf für Netzwerke und Datenzentren zur Speicherung und Auslieferung von Inhalten, Streaming von Videos und deren Produktion, nicht zuletzt auch bei der Entsorgung der Geräte, für einen rapide wachsenden Anteil der weltweiten Emissionen von Treibhausgasen mitverantwortlich ist. Jedoch werden Nachhaltigkeit und Digitalisierung sowie KI noch selten zusammen betrachtet, geschweige denn ethisch reflektiert. Während wir uns über ökomoralische Fragen wie „Soll man noch fliegen, Auto fahren und Fleisch essen?" ▶

[1] Die o.g. Werte basieren auf einer im Rahmen des BMBF-Forschungsprojekts „Automatisiertes ELSI-Screening & Assessment-Tool für MTI-Forschungsvorhaben (ELSI-SAT)" erfolgten Analyse einschlägiger Publikationen zur Ethik der Digitalisierung.

Gedanken machen und von „Flug-Scham“ erzählen, erscheint uns das Digitale immateriell und damit gleichsam umweltneutral. Künstliche Intelligenz als Schlüsseltechnologie der Digitalisierung wird erstaunlicherweise nicht mit dem Narrativ der „Digital-Scham“ assoziiert.

Gegen die „Flut der Ignoranz“ solcher Risiken können eine reflektierte Haltung und entsprechende Vorgehen in der Praxis hilfreich sein. Dazu bedarf es der Verständigung und Sensibilisierung sowie eines für die Praxis tauglichen Ethics-by-Design-Ansatzes. Diese drei Schritte sollen im Folgenden näher erläutert werden.

Verständigung

Erfahrungsgemäß verwenden wir häufig die Begriffe so, als würden wir alle dasselbe darunter verstehen. Gleichwohl lehrt uns die Praxis, auch die wissenschaftliche, dass je nach Herkunft, Erfahrungskontext und Perspektive sehr wohl unterschiedliche Bedeutungen mit einem Begriff assoziiert werden. Insbesondere bei Werten kann die semantische Auffüllung des jeweiligen Begriffs differieren. So ist Vertrauen aus Sicht der Techniker an die Beweiskraft eines funktionierenden Systems gebunden, während aus philosophischer Sicht Vertrauen, wenn sie eines Beweises bedarf, kein Vertrauen mehr ist. Vertrauen meint in letzterem Sinn ein Sich-Verlassen auf ein Gegenüber angesichts eines ungewissen und risikohaften Ausgangs einer Handlung. Es ist also sinnvoll, sich im Vorfeld einer Wertereflexion und einer ethischen Folgenabschätzung über die zentralen Begriffe zu verständigen. Ein probates Mittel hierfür ist es, Menschen ihre Erfahrungen und Erlebnisse (einander) erzählen zu lassen und damit deren jeweiliges Verständnis für alle sichtbar zu machen. Der Vorteil eines solchen narrativen Ansatzes besteht darin, nicht vordergründige Einstellungen und Meinungen der Beteiligten, sondern tieferliegende Bedeutungen zu ermitteln, die sich aus deren Erfahrungen und Erlebnissen abstrahieren lassen.

Für eine Verständigung bedarf es gleichwohl auch der kritischen Auseinandersetzung mit Begriffen. Künstliche Intelligenz (KI) ist das beste Beispiel dafür. Eine Analyse der gängigsten Definitionen von KI zeigt, dass KI fast immer mit Attributen beschrieben wird, die diese vermenschlicht: Es ist von „Lernen“, „Verstehen“, „Entscheiden“, „Wahrnehmen“ und „Probleme lösen“ die Rede. KI wird also anthropomorphisiert oder zumindest „Menschenähnlichkeit“ attestiert. Der Begriff „Künstliche Intelligenz“ suggeriert, dass eine dem Menschen vergleichbare Intelligenz existiert. Das ist allerdings nicht der Fall. Bewusstsein und Gefühle sind Charakteristika, die dem Menschen vorbehalten sind. Auch wenn unklar ist, wie Bewusstsein entsteht und was Bewusstsein eigentlich ist, kann derzeit nicht davon ausgegangen werden, dass Maschinen zur Selbstreflexion fähig sind und ein „Ich“, also eine eigene Identität, ausbilden können. Noch viel weniger sind sie in der Lage, unbewusst etwas zu verdrängen, wie es der Mensch nur allzu gerne tut. Auch über Emotionen verfügen Maschinen nicht, wenngleich sie zu deren Imitation bereits fähig sind. Sie haben auch keinen freien Willen und keine biologischen Körper. Sie verarbeiten zwar selbstständig Daten, was als sogenanntes „Maschinelles Lernen“ beschrieben wird, aber sie lernen nicht wie wir Menschen, die im sozialen Miteinander, aus der Erfahrung von Freude und Leid und aus Vernunftgründen lernen. Maschinen sind (bislang) auch keine Generalisten, sondern Spezialisten – sie können nicht wie der Mensch gleichzeitig über verschiedene Fähigkeiten verfügen, also sich ein Kochrezept ausdenken, eine Oma trösten, ein Musikstück komponieren und ein Bild malen. Gleichwohl kann der Computer „Watson“ Kochrezepte entwickeln, der Pflegeroboter „Mario“ kann sich um pflegebedürftige Senioren kümmern, die Music-Software „Amper“ kann einen Song komponieren und der Algorithmus von deppart.io kann ein Kunstwerk malen. Menschen können Regeln brechen und unlogisch handeln. Sie können moralische Prinzipien erkennen und auf sich selbst anwenden und handeln moralisch aufgrund ihres Gewissens. Maschinen haben kein Gewissen und können keine Verantwortung übernehmen. Aber ganz wesentlich ist: Menschen sind zur Autonomie befähigt, während Maschinen nur autonom Informationen verarbeiten. Autonom ist die KI erst dann, wenn sie nicht mehr auszuschalten ist.

Sensibilisierung für ethische Fragen

Wie mittels Geschichten für ethische Konflikte der Digitalisierung sensibilisierte werden kann, zeigt beispielsweise das Projekt „Die 10 Gebote der Digitalen Ethik“[2] (Abb. 2). Zu jedem Gebot wird eine Geschichte erzählt. Die Gebote und Alltagsgeschichten sollen einen Impuls geben, sich mit ethischen Fragen zu befassen. In den ersten beiden Geboten geht es um den Schutz der Privatsphäre, dann darum,

[2] Die „10 Gebote der Digitalen Ethik“ sind im Institut für Digitale Ethik in einem Masterprojekt mit Studierenden in Kooperation mit Wolfgang Schuster (Telekom-Stiftung) und juuuport.de entstanden und mittlerweile in mehrere Sprachen übersetzt worden. Online verfügbar unter: https://www.hdm-stuttgart.de/digitale-ethik/digitalkompetenz/10_gebote. Seit Juni 2020 gibt es eine Neuauflage mit aktualisierten Geschichten.

wie ich mir meine Meinung bilde, ohne manipuliert zu werden, und schließlich um Empathie, Achtsamkeit und Selbstschutz sowie die Befähigung, sich auch mal eine Auszeit zu nehmen, also Zeit für Muße und Reflexion zu haben. In einer Geschichte geht es um die Fähigkeit, die eigene Privatheit zu schützen:

*Marie liebt Yoga. Ihre Morgenroutine übt sie am liebsten auf ihrem Balkon aus. Sie teilt Fotos und Videos davon auf Instagram und verlinkt dort regelmäßig ihren Standort. Marie freut sich, dass die Zahl der Follower*innen auf ihrem öffentlichen Instagram-Profil wächst. Seit Kurzem erhält sie jedoch immer häufiger Nachrichten von einem Follower, der sie unbedingt kennenlernen möchte. Marie ist etwas mulmig zumute und blockiert nach weiteren aufdringlichen Nachrichten den Unbekannten. Eines Abends kommt sie nach Hause und ein Mann wartet vor ihrer Tür. Er bedrängt sie so lange, bis eine Nachbarin zu Hilfe eilt. Nachdem der Mann die Flucht ergriffen hat, dämmert es Marie: Das war der aufdringliche Follower! Sie erstattet Anzeige bei der Polizei. Die Polizei fasst den Stalker kurz darauf mit Hilfe der Instagram-Nachrichten und -Fotos, die Marie über ihn gesammelt hat. Marie beschließt in Zukunft keine Beiträge mehr zu posten, die Aufschluss über ihren Wohnort oder aktuellen Aufenthaltsort geben.*

Ethische Reflexionsfragen lassen sich anhand dieser Narration auf vielfältige Weise ableiten, wie beispielsweise: Warum soll ich meine Privatheit schützen? Wie kann ich mich schützen? Wie soll ich mich verhalten, wenn ich einerseits in den Sozialen Medien präsent sein will, andererseits mir aber Privatheit wichtig ist (privacy paradox)? In welchen Bereichen ist meine Privatheit noch gefährdet? Was heißt eigentlich „Privatheitskompetenz (privacy literacy)? Sollten Soziale Medien Verantwortung übernehmen, um meine Privatheit zu schützen? Und wie müssten solche Plattformen gestaltet sein, dass sie mich schützen?

Das Projekt „10 Gebote der Digitalen Ethik“ ist vor allem darauf angelegt, die individuellen Kompetenzen der Nutzer*innen zu stärken. Für Unternehmen und Organisationen sind hingegen alternative Instrumentarien zu wählen. Ein Ansatz hierfür ist der des Ethics by Design.

Ethics by Design und Ethical Screening & Assessement

Ethics by Design setzt eine Kooperation von Technologie und Ethik voraus, die während des gesamten Ideen- und Entwicklungsprozesses besteht. Es geht also um die Frage: Wie kommt die Ethik in den Entwicklungsprozess und in das zu entwickelnde Produkt? Die Implementierung von Ethik in den Entwicklungsprozess geschieht mithilfe eines wertebasierten Ansatzes. Ethics by Design heißt, dass ethische Überlegungen von vorneherein angestellt werden, die Diversität der Nutzenden berücksichtigt wird und Grundsätze für ethisches Handeln, beispielsweise in der Herstellung von Produkten, eingehalten werden. Es handelt sich dabei nicht um eine einmalige oder punktuelle Angelegenheit. Ein Produkt, ein Prozess oder ein Handeln wird nicht als „einmal ethisch – immer ethisch“ abgenickt, vielmehr begleitet die Reflexion die Entwicklung und ist auch nach Marktreife des Produktes nicht abgeschlossen.

Die Relevanz einer ethischen Folgenabschätzung lässt sich am Beispiel der Corona-Warn-App, mit der die Bundesregierung die Hoffnung verbindet Infektionsketten möglichst schnell erkennen und stoppen zu können, nachvollziehbar darstellen. Zweck dieser App ist es, dass Menschen, die Kontakt zu infizierten Personen hatten, nicht Gefahr laufen unbewusst das Virus weiterzuverbreiten. Datenschutz und technische Funktionen wurden während des gesamten Entwicklungsprozesses vielfach thematisiert und führten schließlich zu der Entscheidung, einen dezentralen Ansatz zu favorisieren. Aber kaum jemand hatte sich im Entwicklungsprozess darüber Gedanken gemacht, wie die App in einem funktionierenden Gesamtprozess eingebettet ist und die darin relevanten Werte in Bezug auf alle Betroffenen berücksichtigt werden: Welche konkreten Folgen entstehen bei einem Alarm für App-Nutzende, Familie, Angehörige, Ärzte, Gesundheitsämter, Arbeitgeber und Kommunalpolitik? Welche konkreten Anwendungsszenarien lassen sich antizipieren und welche Wertekonflikte können dabei entstehen?

Um Vertrauen in die Corona-Tracing-App zu schaffen, sollte sie nicht nur als technisches Werkzeug betrachtet werden, sondern auch als ein Eingriff in das Leben jedes Individuums. Deshalb ist ein Blick durch die „ethische Brille“ unabdingbar. Dabei hilft der Ethics-by-Design-Ansatz. Das bedeutet: Bereits bei der Konzeption und Entwicklung eines Produkts müssen Werte und ethische Fragestellungen eine entscheidende Rolle spielen. Master-Studierende haben sich in einem Think Tank zusammen mit dem Institut für Digitale Ethik der Hochschule der Medien mit ▸

diesem ethischen Ansatz zur Corona-Warn-App beschäftigt und eine sogenannte Value Map (Abb. 3) erstellt. Als Impuls für eine Debatte wurden fünf Fragen zur Verantwortlichkeit und Fürsorgepflicht von Entwicklern und öffentlicher Hand gestellt:

- Sind die Prozesse im Gesamtsystem so gestaltet, dass sie Vertrauen, Wertschätzung und Verantwortungsgefühl implizieren?
- Ist die Kommunikation rund um die App auf Transparenz und Offenheit hin angelegt?
- Sind genügend Ressourcen vorhanden, um vor allem bei einem positiven Alarm medizinische und psychosoziale Unterstützung für Betroffene zu leisten?
- Wie gelingt die Inklusion möglichst vieler Gesellschaftsgruppen und eine Barrierefreiheit im Gesamtsystem (zum Beispiel bei Sprachbarrieren, technischer Unerfahrenheit und nicht vorhandener Technik)?
- Wie können und sollen Minderjährige mit der App umgehen?

Diese Fragen basieren auf der Value Map zur Corona-Warn-App, die wiederum Ergebnis eines Ethical Screening & Assessement-Prozesses ist. Hierbei werden narrative Mikro-Szenarien entwickelt, die aufzeigen sollen, welche Situationen, Perspektiven, Motive und möglichen Konflikte bei der Nutzung der Corona-Warn-App entstehen können. Aus den Szenarien lassen sich dann zentrale Werte abstrahieren, die sich in einer Übersicht systematisieren lassen: Als Core-Werte stehen das Leben und die Gesundheit aller im Zentrum der Value Map. Voraussetzung für das Gelingen und die Bereitschaft möglichst vieler Nutzer*innen die App zu verwenden, ist das Vertrauen bezüglich ihrer Sinnhaftigkeit, Funktionalität, Datenschutz-Garantie und Offenheit (in technischer und diskursiver Hinsicht). Um dieses Vertrauen herzustellen, bedarf es der Verantwortung des Staates und der Entwickler: Erwartet wird von ihnen eine ständige transparente Information, eine Garantie für vertrauenswürdige Prozesse, die Bereitstellung einer ausreichenden Infrastruktur (insbesondere hinsichtlich der personellen Ressourcen für die Gesundheitsämter und für eine Beratung), ein hoher Standard beim Datenschutz und die Ermöglichung von *Fürsorge* durch die Länder, Landkreise, Kommunen, Gesundheitsämter für die Nutzer*innen, was beispielsweise die Testkapazität, Beratungskapazität, medizinische und psychosoziale Hilfsangebote betrifft. *Verantwortung* müssen aber auch die Nutzer*innen selbst übernehmen. So unterliegen sie zwar keinem Zwang die App zu nutzen, wie dies in anderen Staaten der Fall ist, sie besitzen also *Entscheidungsfreiheit*, aber sie stehen gerade aufgrund dieser Freiheit auch in der Verantwortung sich eine Haltung anzueignen und den Schutz anderer in ihrem Verhalten zu reflektieren: Ob *Gemeinsinn* beziehungsweise *Solidarität* oder Eigensinn stärker wiegen, stellt womöglich für viele Menschen einen Wertekonflikt dar. Wenn man sich für die App entscheidet, dann übernimmt man wiederum Verantwortung in der Handhabung – zum Beispiel als Infizierter eigenverantwortlich den Meldecode zu aktivieren. Wird man gewarnt, ergeben sich für den Betroffenen aber auch eine Reihe an Fragen, wie folgendes Szenario zeigt: *Die App schlägt Alarm. Ich hatte Kontakt mit einer infizierten Person. Was jetzt? Muss ich mir Sorgen machen? Wo finde ich Informationen, wie ich mich verhalten soll? Soll ich beim Gesundheitsamt anrufen? Wie lange hänge ich in der Warteschleife? Bekomme ich schnell einen Test? Begebe ich mich in Quarantäne? Was ist mit meiner Familie und meinen Freunden? Wo bekomme ich psychologische Hilfe? Droht ein mögliches Arbeitsverbot oder gar eine Betriebseinstellung des Unternehmens, bei dem ich beschäftigt bin?* Abgesehen von der nötigen Infrastruktur und Ausstattung, die für ein gelingendes Management der Situation entscheidend sind, ist demnach auch die persönliche Situation der Betroffenen zu berücksichtigen. So stehen diese möglicherweise vor dem Konflikt einerseits verantwortlich handeln zu wollen und sich in Isolation zu begeben und andererseits die sozialen Kontakte unbedingt aufrecht erhalten zu wollen. Auch die Angst vor einem möglichen Arbeitsverlust oder einer Benachteiligung kann mit dem Wunsch, solidarisch zu handeln, konfligieren.

Ein weiterer Schlüsselwert ist die Inklusion, die wiederum in der Verantwortung des Staates und der Entwickler liegt: Wie gelingt eine Teilhabe auch derjenigen, die kein Smartphone besitzen oder nicht über ausreichende technische Kenntnisse zur Handhabung der App verfügen? Wie kann eine Barrierefreiheit bei allen Prozessen (etwa durch fremdsprachige Hotlines) garantiert werden? Und sollen Minderjährige ebenfalls Zugang haben? Wenn ja, wie ist dann die Handhabung in Schulen mit Handyverbot zu regeln? In einer Gesamtschau zeigt sich, dass die Perspektiven aller Akteure und deren Interessen berücksichtigt werden sollten, um ein werteorientiertes Design der App zu ermöglichen.

Wenn sich Unternehmen für eine werteorientierte Strategie der Digitalisierung entscheiden, sollten sie sowohl personenbezogene als auch systembezogene Anforderungen berücksichtigen: 1. Die Beschäftigten sollten in ethischen Fragen der Digitalisierung qualifiziert werden. 2. Die Entscheider sollten für eine Wertehaltung sensibilisiert werden und Anreize für ein verantwortungsvolles Handeln im Unternehmen geben. 3. Um sich im Zuge der gesell-

schaftlichen und technologischen Entwicklungen adäquat zu positionieren, müssten sich Unternehmen ethische Expertise für ein Ethical Screening & Assessement ins Haus holen. 4. Um eine vertrauensvolle Strategie der Ethik in ein Unternehmen zu implementieren, sollte Ethics by Design konsequent umgesetzt werden. Mit dieser Agenda würden Unternehmen glaubwürdig eine werteorientierte Haltung zeigen.

Über die Autorin

Dr. Petra Grimm

ist Professorin für Medienforschung und Kommunikationswissenschaft an der Hochschule der Medien in Stuttgart und leitet dort das Institut für Digitale Ethik (IDE). Sie ist Mitglied im Rundfunkrat des SWR, des Beraterkreises „Gesellschaftlicher Zusammenhalt" des Staatsministeriums Baden-Württemberg und im Forschungsbeirat des Bundeskriminalamts.

▶ https://www.hdm-stuttgart.de/digitale-ethik/home

Literatur

BVDW-Studie (2019): Künstliche Intelligenz, Smart Home, vernetzte Gesundheit – Ethik in der Digitalen Wirtschaft. Online: https://www.bvdw.org/fileadmin/user_upload/190911_DMEXCO_Studie_Ethik_Kernergebnisse.pdf.

Friedman, Milton (1970): The Social Responsibility of Business is to Increase its Profits. New York Times Magazine, September 13. Online: http://umich.edu/~thecore/doc/Friedman.pdf.

Fromm, Erich (2018): Den Menschen verstehen. Psychoanalyse und Ethik. München: dtv.

Grimm, Petra/Müller, Michael (2016): Narrative Medienforschung. Einführung in Methodik und Anwendung. Konstanz/München: UVK Verlagsgesellschaft.

Grimm, Petra/Keber, Tobias/Zöllner, Oliver (2019): Digitale Ethik. Leben in vernetzten Welten [=Kompaktwissen XL]. Ditzingen: Reclam.

The European Commission's High-Level Expert Group on Artificial Intelligence (2019): A definition of AI: Main capabilities and scientific disciplines. Online: https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines.

Wagner, Ben (2018): Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping? Online: https://www.privacylab.at/wp-content/uploads/2018/07/Ben_Wagner_Ethics-as-an-Escape-from-Regulation_2018_BW9.pdf.

Anzeige

preeco

Software für Dokumentation, Organisation und Zusammenarbeit im Datenschutz.

preeco bietet Ihnen zahlreiche Funktionen, die über das reine Dokumentieren hinaus gehen. Erstellen Sie Dokumente und Verträge und halten Sie diese aktuell. Arbeiten Sie im Team und nutzen Sie das interne Ticketsystem und unsere Übersichten für ein nachhaltiges und prozessorientiertes Datenschutzmanagement.

Datenschutzschulungen NEU

Schulungsvorlage auswählen, Rahmenbedingungen einstellen und Teilnehmer einladen. Online Datenschutzschulungen sind jetzt schnell und kostengünstig möglich.

ab 45 €*/ Monat

Jetzt kostenlos testen unter
www.preeco.de/bvd

preeco GmbH, Magirus-Deutz-Straße 14, 89077 Ulm, Mo-Fr 9-17 Uhr, Tel. 0731 96589258

MEHR (ALS) DATENSCHUTZ:

Plädoyer für ein planvolles Vorgehen für Datenschutz by Design[1]

Marit Hansen und Benjamin Bremert

1. Einleitung

Im Oktober 2019 legte die Datenethikkommission der Bundesregierung ihr Gutachten vor.[2] Wie zu erwarten war, geht es darin nicht nur um das zweifellos wichtige Thema Datenschutz, sondern es werden weitergehende Fragen, die einen Bezug haben zu Daten, zur Umsetzung ethischer Grundsätze, zur Digitalisierung, behandelt, denn all dies betrifft unsere Gesellschaft und die Menschen. Dreh- und Angelpunkt der Datenethikkommission (DEK) war gar nicht so sehr die Perspektive der Ethik, sondern der Diskurs basierte auf den beruflichen und professionellen Hintergründen und Erfahrungen der DEK-Mitglieder. Ein wichtiges Ergebnis einer jeden Sitzung war die Pluralität der Sichtweisen, die sich trotz ihrer Verschiedenheit immer wieder in weitgehenden Einklang bringen ließen, und das Ringen um Lösungen auf Basis der ausgetauschten Argumente.

Im Datenschutz ist dies eigentlich eine gewohnte Übung: Ständig werden wir konfrontiert mit vermeintlichen Gegensätzen wie „Datenschutz und Sicherheit", „Datenschutz und Freiheit", „Datenschutz und Nutzbarkeit" und so weiter. Aber dies müssen nicht unauflösbare Gegensätze sein. Um verträgliche Lösungen zu entwickeln, ist es jedoch notwendig, die verschiedenen Anforderungen zu kennen und sich möglicher Interdependenzen und Auswirkungen bewusst zu sein, die Einfluss auf die Gestaltung haben. Auch in der Rolle als Datenschutzbeauftragte – selbstverständlich mit dem Fokus auf die Datenschutzpunkte – empfiehlt sich, solche manches Mal nicht oder nicht explizit kommunizierten Anforderungen aufzuspüren, die Einfluss auf die Datenverarbeitung und die technischen und organisatorischen Maßnahmen haben und damit die einen datenschutzfreundlichen Lösungen als besser und andere als weniger geeignet erscheinen lassen.

[1] Die Erstellung dieses Artikels erfolgte im Rahmen des Forum Privatheit, das mit Mitteln des BMBF unter dem Förderkennzeichen 16KIS0747 (Forum Privatheit – Selbstbestimmtes Leben in der Digitalen Welt) gefördert wird.

[2] Gutachten der Datenethikkommission, Oktober 2019, https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf

Nicht zuletzt seit der europäischen Novelle des Datenschutzrechts und Inkrafttreten der DSGVO wird von datenschutzrechtlich Verantwortlichen häufig beklagt, dass ihnen die Berücksichtigung der umfassenden datenschutzrechtlichen Belange eine unbillige Bürde auferlegen würde. Dass datenschutzkonforme Verfahrensausgestaltung dabei nicht nur eine Optimierung von Verfahren darstellen kann, sondern bei einer frühzeitigen Berücksichtigung auch andere wichtige Belange besser berücksichtigt werden können, wird dabei kaum beachtet. So stellen gewichtige Erwägungen wie beispielsweise die Informationsfreiheit oder der Umweltschutz nur im ersten Moment einen Gegensatz zum Datenschutz dar. Weder bedingt die Informationsfreiheit, dass sämtliche personenbezogenen Daten auf Antrag an Dritte herausgegeben werden müssen, noch führt die Berücksichtigung des Umweltschutzes im Verfahrensdesign dazu, dass rechenintensive und damit eher auch ressourcenintensive Datenverarbeitungen wie starke Verschlüsselung nicht mehr eingesetzt werden sollten.

Die datenschutzrechtlichen Vorgaben können sogar dazu verwendet werden, um Verfahren innerhalb einer Organisation insgesamt planvoller und effizienter zu entwickeln und damit bereits im Entwurfsstadium alle erheblichen Belange zu berücksichtigen, sodass später keine kosten- und zeitintensive Implementierung von zunächst übersehenen oder zu spät kommunizierten rechtlichen Anforderungen stattfinden muss, wenn die Entwicklung eigentlich schon abgeschlossen ist. Ein gutes Datenschutzkonzept ist mitnichten ein Selbstzweck, der nur der Erfüllung einer vermeintlich bürokratischen Auflage dient. Ein Verarbeitungsverfahren „mal schnell" nebenbei zu konzipieren, kann zu Problemen führen, die weit über das Datenschutzrecht hinausgehen. Anhand dieses holistischeren und nachhaltigeren Ansatzes sollen im Folgenden einige Beispiele für die Möglichkeiten einer sinnvollen Verfahrensplanung aufgezeigt werden.

2. Spannungsfelder

Informationsfreiheit

Für Behörden stellt Informationsfreiheit eine immer größere Herausforderung dar. Durch immer größeres Bewusstsein in der Bevölkerung nehmen immer mehr Bürger*innen ihr Recht auf Informationsfreiheit wahr und begehren Zugang zu Informationen öffentlicher Einrichtungen. Das stellt einerseits die Behörden vor die Herausforderung diese Informationen aufzubereiten und herauszugeben, es ruft aber auch Dritte auf den Plan, deren Interessen durch ein Informationszugangsbegehren im Einzelfall berührt sein können. Die Behörde kann bei der Einführung neuer Verfahren, etwa im Zuge der Umstellung auf die digitale Akte, Informationsfreiheit by Design berücksichtigen und etwaige Informationen schon im Stadium ihrer „Entstehung" auf eine mögliche Relevanz für Informationszugangsanfragen kategorisieren. Auch die Einbeziehung Dritter an dieser Stelle führt dazu, dass mögliche spätere Anfragen schneller bearbeitet und der durch die Anfrage Betroffene nicht von dem Umstand überrascht wird, dass Daten herausgegeben werden. Im selben Zug kann für die Behörde aber auch relevant sein, ob die Informationen nach Art und Umfang möglicherweise gar nicht auf Anfrage im Einzelfalls herausgegeben werden, sondern bereits im Vorfeld proaktiv veröffentlicht werden sollten. Einige landesrechtliche Regelungen schreiben eine proaktive Veröffentlichung vor, aber natürlich kann im Sinne einer verbesserten Transparenz des Verwaltungshandelns eine öffentliche Stelle auch von sich aus bestimmte Informationen offenlegen. Durch einen systematischen Ansatz, in dem Informationsfreiheit by Design bei der nach Artikel 25 DSGVO verpflichtenden Gestaltung im Sinne von Datenschutz by Design von Anfang an Berücksichtigung findet, kann möglichen Konflikten vorgebeugt werden.

Umweltschutz

Mit einer ähnlichen Herangehensweise lassen sich auch Umweltaspekte bei der Konzeption neuer Verarbeitungsverfahren wirksam berücksichtigen. So kann etwa die Implementierung eines durchdachten Kryptokonzeptes dafür sorgen, dass ein nach dem Stand der Technik wirksamerer und effizienterer Verschlüsselungsmechanismus verwendet wird. Die systematische Abbildung von Verarbeitungsverfahren und die Planung der für den Betrieb der Datenverarbeitung notwendigen Ressourcen kann aber auch dafür verwendet werden, um (etwa durch Virtualisierung) eine dynamische und ressourcenschonende Technikinfrastruktur zu verwenden. Der Betrieb eines optimierten Verfahrens auf einer Plattform, die performant läuft und der abhängig von der Last im konkreten Zeitpunkt mehr oder weniger Ressourcen zugeteilt werden, lässt sich durchaus in Einklang mit dem Datenschutz bringen. ▸

Weniger Datenverarbeitung – ganz im Sinne der Datenminimierung – bedeutet auch weniger Energieverbrauch. Schwieriger ist die Bestimmung der Umweltauswirkungen bei datenschutzfreundlichen Verfahren, deren Schutz darin besteht, dass zusätzliche Parteien, etwa als Treuhänder oder als Abschottung gegen eine potenzielle Verknüpfung von Daten, einbezogen werden. Wiederum verbraucht eine Datenverarbeitung im Endgerät (und damit mit einer höheren Kontrollmöglichkeit durch die Nutzenden) weniger Energie, als wenn alle Daten standardmäßig über das Internet in große Cloud-Systeme gesandt werden. Manchmal vernimmt man das Kostenargument, es sei günstiger, die Datenverarbeitung dort ablaufen zu lassen, wo die Energie billig ist. Das ist allerdings noch kein Umweltargument; eine Korrelation zwischen Energiepreis und Umweltfreundlichkeit der Energiebereitstellung liegt gerade nicht vor.

Manchmal kommt man mit der Datenschutzbrille aber auch nicht sofort darauf, dass eine Maßnahme eine Auswirkung auf die Umwelt haben könnte: So hat vermutlich keiner aus der Datenschutzszene etwas gegen einen Schredder, der das Papier auch dann ganz besonders klein häckselt, wenn die Papierdaten nicht so sehr sensibel sind. Nur kann daraus resultieren, dass die verbleibenden Schnipsel weniger gut für ein Recycling geeignet sind. Das Umweltsiegel „Blauer Engel" für Aktenvernichter hebt nach Kenntnis der Autoren einen niedrigen Stromverbrauch, die Langlebigkeit der Konstruktion und die Verwendung umweltschonender Materialien hervor – das alles sind wichtige Eigenschaften, die nicht im Spannungsverhältnis zu Datenschutzanforderungen stehen. Zur Recyclingfähigkeit des Schredderguts werden meist keine Aussagen getroffen.

Datenzugang

Internet of Things, vernetztes Fahren, Smart Homes – ein ständiger Strom von Daten wird benötigt, um die Geräte und Verarbeitungen zu steuern und zu optimieren. Große Anbieter sammeln Daten der Kund*innen – datenschutzkonform mit Rechtsgrundlage, vielleicht auch frühzeitig anonymisiert zu Zwecken der Weiterverwendung. Sie können damit abgesicherte Systeme aufbauen und ihrer Verantwortung nach der Datenschutz-Grundverordnung nachkommen. Aber daraus kann auch eine ungewünschte Monopolisierung resultieren. Beispielsweise moniert die Bundesfachgruppe Freie Werkstätten des Deutschen Kfz-Gewerbes, dass die bisherigen Konzepte ihnen keinen fairen Zugang zu den Daten des vernetzten Zugangs bieten.[3] Auch Versicherungen äußern ähnliche Kritik. Hier sollen die Vor- und Nachteile der verschiedenen Konzepte nicht ausgeführt werden, jedoch zeigt sich ein Bedarf an einem Interessenausgleich, der natürlich auch die Interessen der betroffenen Personen berücksichtigen muss. Eine abgesicherte Zentralspeicherung bei einer einzigen Partei, die datenschutzkonform realisiert werden könnte, wird dies vermutlich weniger geeignet umsetzen können als ein föderiertes System von Treuhändern, die sich fein austarierten und technisch oder rechtlich durchsetzbaren Spielregeln unterwerfen.

Transparenz

Ein weiterer Aspekt, der während der Entwicklung der Tracing-Anwendung im Zuge der SARS-CoV-2-Pandemie deutlich wurde, sind die positiven Auswirkungen von Transparenz und Open Source. Gerade eingriffsintensive Datenverarbeitung kann durch einen transparenten Umgang mit den Datenverarbeitungsverfahren eine bessere Akzeptanz erfahren. Falsch ist in diesem Zusammenhang die Annahme, dass eine quelloffene Softwareentwicklung zu einer unsicheren Software führt. Nur durch offenen Quellcode können Dritte (wie Sicherheitsforscher*innen) etwaige Lücken auf legalem Wege entdecken und so zu einer besseren Informationssicherheit beitragen. Die eigene Sicherheit dabei maßgeblich darauf fußen zu lassen, dass Quellen und Funktionsweisen nicht offen sind, also sogenannte „security through obscurity", kann in keinem Fall zu einem wirklich sicheren System führen.

Es ist dadurch aber auch möglich, dass Nutzer*innen selbst oder mit Hilfe von Expert*innen oder Prüfeinrichtungen, denen sie Vertrauen entgegenbringen, die konkreten Datenverarbeitungsvorgänge und so auch die Eingriffsintensivität besser einschätzen können. Das beste Vertrauen basiert auf einer Vertrauenswürdigkeit der Gestaltung. Gerade in sensiblen Bereichen kann man durch überobligatorische Offenheit für Vertrauen sorgen.

Wirtschaftlichkeit

Häufig wird beklagt, dass eine datenschutzrechtskonforme Ausgestaltung von Verarbeitungsverfahren zulasten der Wirtschaftlichkeit gehen würde. Einerseits beruht diese Einschätzung teilweise auf

[3] https://www.kfzgewerbe.de/presse/pressemeldungen/freie-werkstaetten-fordern-fairen-zugang-zu-daten.html

dem Umstand, dass ein oder mehrere Datenverarbeitungsverfahren schon vor Inkrafttreten der DSGVO implementiert und zu diesem Zeitpunkt dem Datenschutz kaum Relevanz beigemessen wurde. Dabei wird auch verkannt, dass viele Pflichten bereits vor Inkrafttreten der DSGVO bestanden und sich an den wesentlichen Kriterien der datenschutzrechtskonformen Ausgestaltung von Verarbeitungsverfahren im Kern nicht so viel geändert hat. Gerade in einer Zeit, in der Datenpannen und Vorfälle im Bereich der IT-Sicherheit erhebliche Konsequenzen haben können, einerseits in Bezug auf negative Berichterstattung und andererseits in Bezug auf zivilrechtliche Ansprüche durch Betroffene, sollte die konforme Verfahrensausgestaltung nicht nur im Eigeninteresse stattfinden, sondern sie kann auch als Wettbewerbsvorteil genutzt werden. So werden nach einer Umfrage Unternehmen von Verbraucher*innen bevorzugt, die die personenbezogenen Daten der Kunden schützen. Der Aspekt ist demnach in sämtlichen Märkten das zweitwichtigste Auswahlkriterium nach der Qualität von Produkten und Dienstleistungen.[4]

3. Umsetzung

Es bleibt die Frage, wie Verantwortliche ihre Verarbeitungsverfahren planvoll konzipieren, implementieren und betreiben können. Die Berücksichtigung der Prinzipien der DSGVO führt bereits dazu, dass sich der Verantwortliche eingehend mit den Verarbeitungszwecken, den Mitteln der Verarbeitung und den dafür notwendigen personenbezogenen Daten beschäftigen muss. Dafür müssen Verarbeitungsverfahren sinnvoll umgesetzt, und die Umsetzung an den formellen Pflichten der DSGVO ausgerichtet werden. Diese Pflichten, wie etwa die Erstellung eines systematischen Verarbeitungsverzeichnisses, dienen den Verantwortlichen zwar auch zum Nachweis der Compliance gegenüber den Aufsichtsbehörden, sie führen aber im Idealfall dazu, dass sich Verantwortliche intensiver mit der eigenen Datenverarbeitung beschäftigen müssen, die technischen Abläufe kennenlernen und Designentscheidungen gerade im Hinblick auf die Risikobeurteilung hinterfragen. Das kann allerdings nur dann erreicht werden, wenn die Dokumentationspflichten nicht nur oberflächlich durchgeführt werden, sondern stets so tiefgehend, wie dies unter Berücksichtigung der Eingriffsintensivität im konkreten Fall und den daraus resultierenden Risiken für Grundrechte und Grundfreiheiten betroffener Personen geboten ist. Da die Erkennung dieser Risiken maßgeblich von der Darstellung der Verarbeitung abhängt[5], muss bereits hierbei auf ausreichende Detailtiefe und Verständlichkeit gedrängt werden, auch wenn es sich nicht um eine Verarbeitung personenbezogener Daten im Hochrisikobereich handelt.

Mögliche Probleme treten bei der systematischen Darstellung dann auf, wenn die Datenverarbeitung auf geschlossene Software- oder Hardware-Komponenten Dritter zurückgreift oder bei der Verarbeitung auf Schnittstellen Dritter für die Verarbeitung personenbezogener Daten zurückgegriffen wird. Über die konkrete dort stattfindende Verarbeitung haben die Verantwortlichen häufig wenig Kenntnis, sodass sogar die Gefahr besteht, dass Daten Dritten gegenüber offenbart werden[6]. Von der Weitergabe von Daten abgesehen, könnten derartige Komponenten über undokumentierte Funktionen verfügen[7] oder dokumentierte Funktionen nicht ordnungsgemäß funktionieren. Dieser möglichen Schutzlücke kann durch Sicherstellung lückenloser Compliance begegnet werden. Bei maßgeschneiderter Software oder Bibliotheken dürfen sich Verantwortliche bis zu einem gewissen Zeitpunkt darauf verlassen können, dass sich in geschlossener Soft- und Hardware nur die Funktionalität befindet, die auch bestellt wurde. Anders verhält es sich jedoch dann, wenn Verantwortliche einen konkreten Verdacht haben, dass genutzte Komponenten nicht wie erwartet funktionieren oder Daten anders oder weitergehend verarbeiten. Je nach Eingriffsintensivität kann es, gerade auch bei der Datenverarbeitung öffentlicher Stellen, erforderlich sein, dass sich die Verantwortlichen von der konkreten Funktionalität und Funktionsweise durch Vorlage des Quellcodes überzeugen.

Denkt man nun etwas größer, fällt auf, dass in anderen Bereichen der Digitalisierung ein ähnlich stabiles regulierendes Fundament, wie es die DSGVO mit sich bringt, fehlt. Nötig ist daher eine Weiterentwicklung des Rechtsrahmens zur Beherrschung von risikoträchtigen Verfahren außerhalb der Verarbeitung personenbezogenen Daten. Die DSGVO kann dies naturgemäß nicht leisten, aber gibt mit den Datenschutz-Grundsätzen und der Orientierung am Risiko einen Maßstab vor, der sich übertragen lässt. Dies war ebenfalls ein Arbeitspunkt der Datenethikkommission. Um nur ein Beispiel zu nennen, schlägt die Datenethikkommission für ▸

[4] The Harris Poll, IBM Cybersecurity and Privacy Research, 13.04.2018, S. 13, online abrufbar unter: http://newsroom.ibm.com/Cybersecurity-and-Privacy-Research

[5] Bieker/Bremert, in: Identifizierung von Risiken für die Grundrechte von Individuen: Auslegung und Anwendung des Risikobegriffs der DS-GVO, ZD 2020, 7, 8f.

[6] Vgl. im Falle von Facebook-Apps: CNBC, Facebook reportedly gets deeply personal info, such as ovulation times and heart rate, from some apps, 22.02.2019, online abrufbar unter: https://www.cnbc.com/2019/02/22/facebook-receives-personal-health-data-from-apps-wsj.html

[7] Wagner/Salzmann, in: IT-Sicherheit im Internet of Things: Überwachungspotenzial smarter Küchenhelfer, ZD-Aktuell 2019, 06731; Kleine Anfrage von Abgeordneten der Fraktion der SPD zum „Einsatz der Quellen-Telekommunikationsüberwachung", BT-Drs. 17/11598, S. 9ff.

algorithmische Systeme – auch ohne Personenbezug – fünf Stufen vor, deren Risiken mit den für die Kategorien passenden Maßnahmen angemessen eingedämmt werden müssen (siehe Abb. 1). Dass hier zeitiger Regulierungsbedarf besteht, ist mittlerweile auch auf der europäischen Ebene akzeptiert.

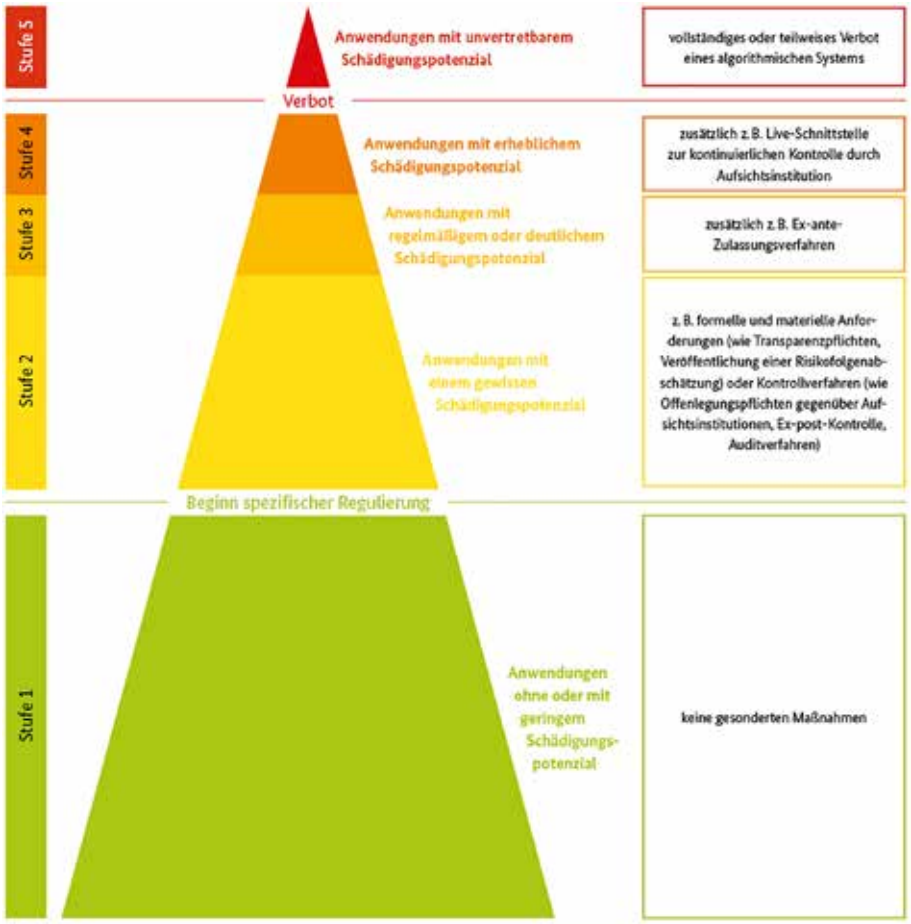


Abb. 1: Kritikalität und risikoadaptiertes Regulierungssystem für algorithmische Systeme[8]

4. Fazit

Mehr Datenschutz – das wollen wir. Es wird manchmal der Eindruck erweckt, dass „Datenschutz first" ein längst gelebtes Prinzip sei, das mit anderen Anforderungen und Grundwerten kollidiert, ja, diese quasi diskriminiert und klein macht. Weder das eine noch das andere kann das Autorenteam bestätigen: Es besteht immer noch Nachholbedarf, was Datenschutz in Technik und Organisation betrifft. Und der Slogan vom „Datenschutz als Verhinderer" ist ebenfalls falsch (es sei denn, die Verarbeitung ist datenschutzrechtlich unzulässig – dann muss sie natürlich unterbleiben). Was aber stimmt: Mit Einführung der DSGVO ist Datenschutz stärker ins Bewusstsein gerückt, und das Thema „Datenschutz by Design" nimmt – endlich – Schwung auf. Empfohlen sei aber die Weitung der Perspektive auch für andere Rechte und Freiheiten von Menschen, für das Gemeinwohl und für Fairness in der Gestaltung der Verarbeitungen.

Ein Ansatz, der mehr im Blick hat als „nur" Datenschutz, bedeutet nicht, die Datenschutzanforderungen weniger zu beachten. Jedoch können dann Lösungen vermieden werden, die sich lediglich auf die Datenschutzumsetzungen konzentrieren und damit – als unabsichtlichem Nebeneffekt – die Wahrnehmung anderer Rechte erschweren. Im Bestfall entwickelt sich daraus im Laufe der Zeit eine einheitliche Verfahrensweise auf Basis grundsätzlicher abstrakter Erwägungen aus dem Planungsstadium, und dies wird zum Bestandteil der bei allen Verantwortlichen gelebten Kultur. Denn darum geht es doch: Um die zukunftsfähige und nachhaltige Entwicklung unserer Gesellschaft, in der die Digitalisierung eine unterstützende Rolle spielt, statt zu einer Bedrohung zu werden.

[8] Gutachten der Datenethikkommission, Oktober 2019, S. 177.

Über die Autoren

Marit Hansen
ist Landesbeauftragte für den Datenschutz Schleswig-Holstein und damit Leiterin des Unabhängige Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Dort begann die Informatikerin ihre Laufbahn ab 1995 zunächst als Referentin und Referatsleiterin. Marin Hansen war Mitglied in der Datenethikkommission der Bundesregierung und erhielt im April 2020 für ihre Verdienste in datenschutzfreundlicher Systemgestaltung die Ehrendoktorwürde der schwedischen Universität Karlstad verliehen.

Benjamin Bremert
ist juristischer Mitarbeiter im Projektreferat des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) und Mitglied im Forum Privatheit.

▶ www.datenschutzzentrum.de

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

KONTROLLE UND HAFTUNG BEI ALGORITHMISCHEN SYSTEMEN – ANMERKUNGEN ZUM WEISSBUCH DER EU-KOMMISSION

Prof. Dr. Christiane Wendehorst

Algorithmische Systeme gehören unter Bezeichnungen wie „EDV" schon lange zu unserem Alltag. Sie erleichtern uns das Leben in fast allen Bereichen, führen zu mehr Effektivität und ermöglichen technologischen Fortschritt, der wiederum zum Wohl aller eingesetzt werden kann. Dies ist weder neu noch spektakulär. Dass plötzlich der Begriff „Algorithmus" vielfach einen bedrohlichen Klang erhalten hat, liegt an der rasanten Entwicklung, welche algorithmische Systeme in den letzten Jahren genommen haben.

Durch den exponentiellen Anstieg von Rechenleistung, Speicherkapazitäten und Datenmengen ist es möglich geworden, algorithmische Systeme einer ganz neuen Generation zu entwickeln. Wir nennen sie gemeinhin „Künstliche Intelligenz" (KI) und wollen damit zum Ausdruck bringen, dass Maschinen Aufgaben bewältigen können, welche bislang kaum oder gar nicht zu programmieren waren. Bei KI wird nicht mehr regelbasiert programmiert, sondern Maschinen entwickeln mithilfe eigener Lernalgorithmen eigene Lösungswege, welche sich im Einzelnen nicht nachvollziehen lassen, aber frappierende Erfolge aufweisen. Da wird der weltbeste Spieler in GO von einer Maschine geschlagen, vermögen Maschinen treffsicherer als ein Arzt bösartige von gutartigen Hautveränderungen zu unterscheiden, bringen fahrerlose Autos Menschen von A nach B oder hilft Software bei der Personalauswahl.

Der Ruf nach Kontrolle und Haftung

Derartige Erfolge geben Anlass zu Ängsten und Befürchtungen. Auf nationaler, europäischer und internationaler Ebene sind Arbeitsgruppen entstanden, welche sich der Ausarbeitung ethischer und rechtlicher Leitlinien verschrieben haben. In Deutschland gehörte dazu die Datenethikkommission (DEK), die im Sommer 2018 ihre Arbeit aufnahm und im Oktober 2019 ihr Schlussgutachten einreichte. Auf europäischer Ebene ist insbesondere die High Level Expert Group on Artificial Intelligence (AI HLEG) zu nennen, die in mehreren Etappen Richtlinien für vertrauenswürdige KI und politische Empfehlungen erarbeitete. Ein Beispiel für eine internationale Arbeitsgruppe wäre die Global Partnership on AI (GPAI), die erst kürzlich ihre konstituierende Sitzung hatte und Experten aus vielen Kontinenten vereint.

Die EU-Kommission widmete sich dem Thema KI bereits verschiedentlich, jüngst im Februar 2020 im „Weißbuch zur künstlichen Intelligenz", in dem sie ein „Ökosystem für Exzellenz" sowie ein „Ökosystem für Vertrauen" ankündigt. Letzteres soll wirkungsvolle Mechanismen zur Kontrolle algorithmischer Systeme enthalten und für eine angemessene Haftung sorgen, wenn diese Schäden verursachen.

Die ‚physische' und die ‚soziale' Dimension von KI-Anwendungen

Sowohl unsere Hoffnungen und Erwartungen an KI als auch die mit KI-Anwendungen verbundenen Risiken betreffen zwei verschiedene Dimensionen: die „physische" Dimension und die „soziale" Dimension.

In der physischen Dimension erwarten wir von KI sicherere Fahrzeuge, bessere Gesundheits- und Pflegeleistungen und wirkungsvolleren Klimaschutz. Dem stehen physische Risiken gegenüber, insbesondere Tod, Körperverletzung, Sach- oder Umweltschäden, die durch unsichere KI-Produkte und KI-Dienstleistungen verursacht werden. Diese Dimension steht im Vordergrund bei selbstfahrenden Fahrzeugen, Drohnen oder Medizin- und Pflegerobotern und bei Schäden, die durch den Betrieb solcher Geräte verursacht werden können.

Oft handelt es sich um KI, die fest in bestimmter Hardware verbaut ist und die Aktionen dieser Hardware steuert. Während die mit der KI einhergehende Opazität, Komplexität und Unvorhersehbarkeit das von solchen Geräten ausgehende Risiko sicherlich noch erhöhen kann, ist das Risiko als ▸

solches traditioneller Art. Mit anderen Worten: Andere technische Entwicklungen könnten einen ähnlichen Effekt auf das „physische" Risiko haben, und die Auswirkungen auf ein Opfer können die gleichen sein, unabhängig davon, ob der Verkehrsunfall, bei dem es ums Leben kam, durch KI oder durch eine andere Fahrzeugkomponente verursacht wurde.

In der sozialen Dimension erwarten wir von KI bessere und gerechtere Entscheidungen, die Entlastung von Menschen und Schaffung von Freiräumen, wirkungsvollere Verbrechensbekämpfung und ähnliches. Dem stehen wiederum Risiken eher sozialer Natur gegenüber. Dazu gehören Diskriminierung, Überwachung, Manipulation und Ausbeutung durch unangemessene Entscheidungen, die mit Hilfe der KI getroffen wurden.

Die zweite der beiden Dimensionen ist wesentlich KI-spezifischer. Hier geht es um KI, die für Zwecke wie Personalentscheidungen, personalisierte Preisgestaltung, personalisierte Nachrichten-Feeds oder Predictive Policing verwendet wird. Oft handelt es sich um reine Softwarelösungen, bei denen die Hardware, auf denen sie betrieben wird, in den Hintergrund gerät. Während Diskriminierung, Manipulation oder Ausbeutung durch Menschen so alt sind wie die Menschheit selbst, ist die Situation mit KI in verschiedener Hinsicht ganz neu. Menschliche Gehirne sind mit „übermenschlichen" Rechenkapazitäten konfrontiert, was zu extremer Waffenungleichheit und gegebenenfalls zu Kontrollverlust führt. Auch ist Ungerechtigkeit oder Inkompetenz in einem scheinbar „neutralen" und kaum erklärbaren Code verborgen, der vielfach kopiert wird und als Grundlage neuer Codes dient, was bedeutet, dass wir die Fähigkeit verlieren könnten die Probleme zu erkennen und zu korrigieren. Andererseits könnten wir zum ersten Mal in der Lage sein Entscheidungsfindungsverfahren tatsächlich zu analysieren, zu kontrollieren und zu optimieren, da die Kontrolle und Optimierung von Maschinen nicht so leicht in Konflikt mit den Grundrechten gerät.

KI-Anwendungen bedeuten gewöhnlich Herausforderungen sowohl in der physischen als auch in der sozialen Dimension. Zum Beispiel stellen medizinische Entscheidungsunterstützungssysteme ein traditionelles Risiko der Verursachung von Personenschäden dar (und sind daher in der Verordnung über Medizinprodukte enthalten), aber sie können naturgemäß auch die Arzt-Patienten-Beziehung verändern und möglicherweise zur Diskriminierung bestimmter Patientengruppen führen. Bei den meisten KI-Anwendungen liegt der Schwerpunkt eindeutig aber auf einer der beiden Dimensionen, je nachdem, ob es eher um ein „Tun" oder eher um einen „Entscheiden" geht.

Kontrolle und Haftung in der „physischen" Dimension

Diese Einsicht hat wichtige Implikationen für einen EU-Rechtsrahmen für KI. Betrachten wir die physische Dimension der Risiken, so scheint alles darauf hinzudeuten, dass es primär eines „digitalen Fitness-Checks" des geltenden Produktsicherheitsrechts und des geltenden Haftungsrechts und einer entsprechenden Anpassung der geltenden Regelungen bedarf. Dieser „digitale Fitness-Check" darf sich nicht auf die Betrachtung von KI beschränken, sondern sollte generell digitale Ökosysteme, einschließlich Software als solche, die Entwicklung hin zu „Everything as a Service" und die Vernetzung im Internet of Things (IoT) berücksichtigen. So hat der Bericht einer von der EU-Kommission eingesetzten Expertengruppe zur Haftung für neue Technologien gezeigt, dass nur sehr wenige der auftretenden Haftungsprobleme wirklich KI-spezifisch sind.

Sicherlich werden einige KI-spezifische Maßnahmen erforderlich sein. So bedarf es etwa der Entwicklung von technischen Standards für die Sicherheit und Bewertung von selbstlernenden Systemen. Ebenso bedarf es der Erweiterung existierender Regelungen zur Gefährdungshaftung für Anwendungen, bei denen KI das Risiko über die kritische Schwelle ansteigen lässt (beispielsweise können langsame Fahrzeuge wie große Reinigungsroboter im öffentlichen Raum plötzlich ein Risiko darstellen, das mit dem Risiko vergleichbar ist, das früher nur von schnellen Fahrzeugen ausging). Schließlich bedarf es einer neuen Bewertung von Zusammenhängen, die bislang eindeutig mit menschlichem Handeln in Verbindung standen. So ist es überfällig, dass die strikte Haftung für sogenannte Erfüllungsgehilfen (also menschliche Hilfspersonen, die man zur Erfüllung von Pflichten einsetzt) auf den Einsatz von KI ausgedehnt wird.

Die meisten Maßnahmen, die sich mit der physischen Dimension befassen, werden aber wahrscheinlich aufgrund anderer digitaler Entwicklungen als der KI notwendig werden, insbesondere aufgrund der Vernetzung und Komplexität der Systeme sowie ihrer Offenheit (etwa durch Software-Updates oder die Abhängigkeit von bestimmten Cloud-Diensten).

Umgekehrt ist es gegebenenfalls nicht erforderlich, Maßnahmen, die sich mit der „sozialen Dimension"

befassen (wie Informationspflichten, Recht auf Erklärungen oder Inklusivität von Trainingsdaten), unbesehen auf alle KI-Anwendungen auszudehnen, die weitgehend „physische" Risiken bergen. Wir brauchen nicht in erster Linie Hersteller von autonomen Fahrzeugen, die uns auf transparente Weise erklären, welche Menschen sie lieber zu Tode bringen, und die uns nachweisen, dass das Verhältnis der Verkehrsopfer mit heller Hautfarbe genau dem Verhältnis dieser Personen in der Gesamtbevölkerung entspricht. Vielmehr brauchen wir Hersteller, die autonome Fahrzeuge entwickeln, welche überhaupt niemanden verletzen oder töten. Die nicht enden wollende Diskussion um die sogenannten Dilemma-Situationen. in denen ein autonomes Fahrzeug „entscheiden" muss, wessen Leben oder Gesundheit es eher opfert, dürfte relativ wenig zur Klarheit beigetragen haben, da es ja darum gehen muss, schon die Dilemma-Situation an sich zu vermeiden.

Das EU-Parlament arbeitet derzeit an einem Entwurf für eine Verordnung zur KI-Haftung für „physische" Risiken. Die Ende April 2020 vorgelegte erste Fassung sieht eine Gefährdungshaftung für Schäden vor, welche durch „Hochrisiko-KI" verursacht werden. Welche KI-Anwendungen als „Hochrisiko-KI" gelten, soll sich aus einem Anhang ergeben. Haften soll der jeweilige Halter eines Systems, also derjenige, welcher das System unmittelbar für seine Zwecke betreibt. Das kann eine Privatperson sein (zum Beispiel beim Betrieb eines Reinigungsroboters) oder ein Unternehmen. Die erste Fassung des Anhangs stuft ein eher inkonsistentes Sammelsurium von fünf Anwendungen als „Hochrisiko-KI" ein, so etwa alle autonomen Roboter und die ohnehin fast überall schon von einer Gefährdungshaftung erfassten autonomen Fahrzeuge und Drohnen. Es bleibt zu hoffen, dass im Verlauf des Verfahrens dieser Anhang sinnvoll gestaltet und deutlich wird, in welchem Verhältnis diese neue Gefährdungshaftung für KI zur Haftung des Herstellers oder Entwicklers steht: Der Hersteller oder Entwickler ist nämlich derjenige, der die Risiken von KI am ehesten unter Kontrolle hat und sie mit den geringsten Kosten vermeiden kann.

Kontrolle und Haftung in der „sozialen" Dimension

Die „soziale" Dimension von Risiken ist viel KI-spezifischer und viel schwieriger regulatorisch in den Griff zu bekommen. Der vom EU-Parlament erarbeitete Entwurf zu einer Verordnung über KI-Haftung klammert all diese Risiken von vornherein aus und weist sie allfälligen Spezialvorschriften zu, etwa dem Anti-Diskriminierungsrecht oder dem Datenschutzrecht. Diese Rechtsmaterien enthalten jedoch so gut wie keine KI-spezifischen Regelungen und dürften der Herausforderung kaum gewachsen sein. Ein vom EU-Parlament erarbeiteter Verordnungsentwurf zu ethischen Anforderungen an KI löst das Haftungsproblem ebenfalls nicht.

Dass wir die soziale Dimension von KI regulieren und kontrollieren müssen, wird immer deutlicher. Im Ansatz besteht hierzu weitgehend Einigkeit, und ebenso hinsichtlich vieler KI-spezifischer Regelungsziele, beispielsweise zur Sicherstellung der Inklusivität von Trainingsdaten, zur Gewährleistung der Erklärbarkeit von Entscheidungen, zu Informationspflichten und Folgenabschätzung und zur menschlichen Aufsicht. Das Dilemma, mit dem der Gesetzgeber aber derzeit konfrontiert ist, besteht darin einerseits ein ausreichendes Schutzniveau ohne wesentliche Lücken oder Schlupflöcher gewährleisten zu müssen, andererseits aber Rechtsunsicherheit und überbordende Bürokratie zu vermeiden.

In seinem Streben nach der Quadratur des Kreises, ein hohes Schutzniveau zu erreichen und gleichzeitig Unsicherheit und ein innovationsfeindliches Klima zu vermeiden, schlägt das Weißbuch vor, den Anwendungsbereich des künftigen EU-Rechtsrahmens für KI einzuschränken. Ob eine KI-Anwendung einbezogen wird, sollte in erster Linie von dem betreffenden „Sektor" bestimmt werden. Die „Sektoren", die erschöpfend aufgelistet werden sollen, könnten Bereiche wie Gesundheitswesen, Verkehr oder Energie sein. Zweitens muss innerhalb der aufgelisteten Sektoren das von einer bestimmten Anwendung ausgehende Risiko einen bestimmten Schwellenwert überschreiten. Nur wenn beide Kriterien erfüllt sind, wird eine KI-Anwendung dem neuen Rechtsrahmen unterliegen – von Ausnahmen abgesehen. Dadurch soll gewährleistet werden, dass nur wenige, klar abgegrenzte Akteure in der Wirtschaft mit den neuen Anforderungen konfrontiert sind.

Dieser von vornherein sektoral denkende Ansatz steht im Widerspruch zu den Vorschlägen der DEK, die eher empfohlen hat gleichsam „flächendeckend" nach der Kritikalität (also dem Schädigungspotenzial) algorithmischer Systeme zu differenzieren und alle algorithmischen Systeme ab einer bestimmten Kritikalität – und unabhängig davon, ob sie nun zufällig im Sektor Gesundheitswesen, Verkehr, Energie odgl. eingesetzt werden – einem abgestuften Kontrollsystem zu unterwerfen. ▸

Bedarf nach einem kombinierten Regulierungsansatz

Alle Vorschläge, die bislang zur Regulierung der „sozialen“ Dimension von KI und der korrespondierenden Risiken gemacht wurden, gehen von einem Regulierungsmodell aus, welches ich gerne den „PRRP-Ansatz“ nenne (Principles, Requirements, Rights, Procedures) und das etwa bei der DSGVO angewendet wurde: Der Gesetzgeber formuliert Anforderungen, die erfüllt sein müssen, damit eine Tätigkeit rechtmäßig ist. Er kombiniert dabei meist Prinzipien (wie bei den Grundsätzen der Datenverarbeitung in Art. 5 DSGVO), zwingende Anforderungen (wie das Erfordernis eines Rechtsgrundes nach Art. 6 DSGVO), Individualrechte (etwa die Betroffenenrechte) und Verfahren (zum Beispiel Datenschutzfolgenabschätzung, Dokumentation). Dieser Ansatz ist für Anwendungen hoher Kritikalität auch bei KI erforderlich.

Daneben gäbe es aber auch das Regulierungsmodell des „Blacklisting“ (also das Anlegen „schwarzer Listen“), das oft mit einer Generalklausel kombiniert wird. Diese Regelungstechnik wurde bereits erfolgreich etwa bei der Kontrolle missbräuchlicher Klauseln in Verbraucherverträgen und bei unlauteren Geschäftspraktiken angewendet. Sie bedeutet, dass sich der Gesetzgeber hauptsächlich darauf beschränkt, festzulegen, was nicht getan werden darf. Die Hauptnachteile dieses Ansatzes sind: Er neigt durch die Wortwahl dazu, eine „negative Botschaft“ zu vermitteln und es ist relativ schwierig, die missbilligten Praktiken richtig zu formulieren, insbesondere für sensible und unscharfe Bereiche wie Diskriminierung oder Manipulation. Ein großer Vorteil dieses Ansatzes besteht darin, dass er viel zielgerichteter das trifft, was europäischen Grundwerten widerspricht. Der Ansatz macht es auch leichter sich an veränderte Entwicklungen anzupassen, und kann für Innovationen, insbesondere von KMU, und für den Grundrechtsschutz vorteilhafter sein.

Teils als Ergänzung, teils als Alternative zu den vorliegenden Regulierungsvorschlägen sollte der europäische Gesetzgeber daher erwägen, so etwas wie eine Liste „missbräuchlicher algorithmischer Praktiken“ (Unfair Algorithmic Practices, UAP) zu formulieren und sie unter anderem mit Haftungsnormen zu koppeln. Diese würde auf Wirkungen abzielen, die wir auf jeden Fall vermeiden müssen, wenn wir unsere Zukunft lebenswert gestalten wollen: Diskriminierung (unter Berücksichtigung KI-spezifischer Diskriminierungsformen), Ausnutzung von Vulnerabilitäten, Manipulation, Profiling und Scoring in Bezug auf intimste menschliche Merkmale oder totale Überwachung von Menschen sollten jedenfalls von dieser Liste erfasst sein, damit KI das tut, was sie tun soll: dem Menschen dienen.

Über die Autorin

Christiane Wendehorst

ist Professorin für Zivilrecht an der Universität Wien und Präsidentin des European Law Institute (ELI). Sie war Co-Vorsitzende der Datenethikkommission (DEK) und ist Mitglied einer EU-Expertengruppe zu Haftung und neuen Technologien ebenso wie der Global Partnership for AI (GPAI). Sie hat u.a. die deutsche und östereichische Bundesregierung, die Europäische Kommission und das Europäische Parlament zu verschiedensten digitalen Themen beraten.

Anzeige

MOBILE AKTENVERNICHTUNG
AUF HÖCHSTEM NIVEAU – RHENUS P-7

RHENUS OFFICE SYSTEMS

Sicherheit für Ihre Daten – auf dem Stand der Technik

Ab sofort ermöglicht Ihnen unser mobiles Auflöserfahrzeug die datenschutzkonforme Vernichtung von Material der Schutzklasse SK3 auf Sicherheitsstufen bis zu P-7 gem. DIN 66399.

Rhenus Aktenvernichtung bietet Ihnen auch weiterhin die Optionen „stationär“ (SK2/3) und „mobil“ (SK3).

Sie haben Interesse? Wir beraten Sie gern!

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

Anzeige

www.teletalk.de Mai/Juni 2020 27. Jahrgang

TeleTalk

CUSTOMER CARE & SERVICEMANAGEMENT

Neue Märkte.

Neue Branchen.

Neue Kunden für Sie?

TeleTalk - das führende Fachmagazin für Kundendialog, Customer Care und Servicemanagement informiert branchen- und medienübergreifend über alle relevanten Entwicklungen rund um einen erfolgreichen Dialog mit dem Kunden. Neben allen Aspekten eines modernen, multimedialen Kundenservice- und Customer Care Managements, stehen Informationen über neue Produkte, technische Entwicklungen im Mittelpunkt unserer Berichterstattung.

Lernen Sie TeleTalk jetzt kennen!

Hier bestellen Sie das kostenloses E-Paper Abo der TeleTalk für BvD-Mitglieder.
kundenservice@teletalk.de

CORPORATE DIGITAL RESPONSIBILITY – EIN DIGITALETHISCHER KOMPASS

Wie sich die Lücke zwischen gesetzlichen Vorgaben und den Erwartungen an eine verantwortungsvolle Digitalisierung schließen lässt.

Angelika Pauer, Saskia Becke, Daniela Hanauer und Paul Czech

Die digitale Unternehmensverantwortung wächst

Ob personalisierte Medizin, E-Learning, Homeoffice oder autonomes Fahren – digitale Technologien haben längst Einzug in unseren Alltag gehalten. Sie transformieren in rasendem Tempo bestehende Strukturen der Gesellschaft und Wirtschaft. Digitale Informations- und Kommunikationstechnologien (IKT), Blockchain, cyber-physische Systeme und künstliche Intelligenz (KI) haben sich bereits als Schlüsseltechnologien des 21. Jahrhunderts etabliert. Sie verändern unser Verhalten und Denken grundlegend, etwa beim Arbeiten und Lernen, in der Kommunikation oder in der Art, wie wir konsumieren. Über alle Branchen hinweg interessieren sich immer mehr Unternehmen für die Einsatzmöglichkeiten der digitalen Technologien, da diese vielfältige Chancen bieten, neue wirtschaftliche Potenziale zu heben. Allein durch KI-Anwendungen wird sich das deutsche Bruttoinlandsprodukt nach PwC-Prognosen bis zum Jahr 2030 um mehr als elf Prozent steigern lassen.

Doch mit der Digitalisierung sind auch Risiken verbunden. Bei den Diskussionen über die Vor- und Nachteile der digitalen Transformation wer-

den allerdings häufig nur technologische oder wirtschaftliche Aspekte betrachtet. Die gesellschaftliche und soziale Dimension kommt meist zu kurz. Dabei müssen unternehmerische Entscheidungen, gerade wenn sie mithilfe digitaler IKT getroffen werden, ethisch verantwortet werden. Eine breite gesellschaftliche Akzeptanz der neuen Technologien und Geschäftsmodelle kann nur erreicht werden, wenn Unternehmen den digitalen Wandel werteorientiert, verantwortungsvoll und ethisch gestalten – und den Menschen dabei in den Mittelpunkt stellen. In Europa wird ein solcher Umgang mit Daten, digitalen Produkten und Services nachdrücklich eingefordert. Dazu gehört insbesondere der Anspruch auf Transparenz, Privatheit, Sicherheit, Fairness und digitale Selbstbestimmung.

Unternehmen sollten jedoch nicht auf den Gesetzgeber warten, um ihrer wertebasierten Corporate Digital Responsibility (CDR) nachzukommen. Eine proaktive Selbstregulierung ist geraten, nicht zuletzt auch, um einer gesetzlichen Überregulierung vorzubeugen.

Organisationen, die hohe ethische Standards im Umgang mit digitalen Technologien in ihrer Unternehmenskultur verankern, bauen Vertrauen bei ihren Kunden, Mitarbeitern und anderen Stakeholdern auf, begegnen regulatorischen Risiken und vermeiden Reputationsschäden. Ihre Digitalethik trägt damit unmittelbar zum nachhaltigen Unternehmenserfolg bei und verschafft ihnen Wettbewerbsvorteile.[1]

Vor welchen Herausforderungen stehen die Unternehmen?

Digitale Verantwortung zu übernehmen ist für Unternehmen unverzichtbar, denn dies ist die Grundlage für Vertrauensbildung. Kunden, die einem Unternehmen vertrauen, sind eher dazu bereit, Informationen zu teilen, und verhalten sich insgesamt loyaler. Ohne dieses Vertrauen lassen sich die neuen Handlungsoptionen wie beispielsweise Datenauswertungen mittels Big-Data-Technologien oder Dateninterpretation mittels KI nicht vollends ausschöpfen.

Auch Mitarbeiter erachten es als wichtig, dass ihr Arbeitgeber diesbezüglich ethisch vorbildlich handelt und eine entsprechende Reputation in der Öffentlichkeit hat. Sie hinterfragen daher Unternehmensausrichtung und -entscheidungen zunehmend kritisch. Im Zuge der digitalen Transformation von Arbeit steigt darüber hinaus das Bedürfnis nach wertschöpfender Arbeit.

Die Automatisierung von Tätigkeiten, algorithmusbasierte Entscheidungsprozesse und neuartige Mensch-Maschine-Interaktionen werfen zudem eine Reihe komplexer ethischer Fragen auf.

Wie können Unternehmen also vorgehen, um diesem neuen Handlungsfeld gerecht zu werden? Die Praxis zeigt, dass viele Organisationen noch keine umfassende Strategie für digitale Ethik entwickelt haben. So offenbart eine aktuelle PwC-Studie, in deren Rahmen 300 Unternehmensvertreter aus unterschiedlichen Branchen zu diesem Thema befragt worden sind, dass etliche Unternehmen in diesem Zusammenhang nur die technischen Aspekte und die Umsetzung der Datenschutzgrundverordnung (DSGVO) sehen. Digitale Ethik umfasst aber viel mehr als das. PwC hat in diesem Bereich fünf Herausforderungen identifiziert, vor denen die Unternehmen aktuell stehen:

1. Überregulierung versus fehlende Regulierung

Bisher gibt es für die Digitalisierung noch kein Rahmenwerk, das die ethischen Anforderungen adressiert. Damit es in Zukunft nicht zu einer Überregulierung kommt, müssen Unternehmen proaktiv tätig werden und gemeinschaftlich Standards setzen. Wie sehr soll ein jedes Unternehmen selbst Verantwortung übernehmen? Wer ist für Entscheidungen verantwortlich?

2. Datennutzung versus Schutz der Privatheit

Viele technologische Entwicklungen können einen Mehrwert schaffen, sind dabei aber Datenschutzbestimmungen ausgesetzt, die gegebenenfalls Innovationen behindern können. Wie viele Daten ein Unternehmen und eine Technologie nutzen, hängt immer vom Anwendungsfall ab.

Es stellt sich immer die Frage, ob der Nutzen auch den Weg legitimiert. Sollte beispielsweise ein Modell, das Krebs vorhersagen kann, alle Daten von Patienten zur Prädiktion verwenden, also auch etwa Hautfarbe, Ethnizität oder Religion, falls sich hier indirekte Korrelationen ergeben?

3. Automatisierung von Entscheidungsprozessen versus Fairness

Gerade in der aktuellen COVID-19-Krise wird häufig diskutiert, wie Betten auf Intensivstationen im Krisenfall zu vergeben sind. Wäre im Fall einer Triage auf das Alter oder die Schwere der Erkrankung abzustellen? Dies lässt sich auch durch Systeme modellieren und entscheiden. Jede Entscheidung muss begründbar sein. Wie kann das Unternehmen in jedem Fall Fairness und Transparenz sicherstellen, um für automatisierte Entscheidungen die Verantwortung übernehmen zu können?

4. Menschlicher Kontakt versus Einsatz von KI

Dienstleistungen werden zunehmend mithilfe von Chatbots automatisiert. Gleichzeitig wünschen sich Menschen immer mehr einen persönlichen Kontakt. ▸

Wie können Unternehmen bei Wahrung der Transparenz hier Lösungen finden, die Vertrauen schaffen und gleichzeitig nicht „Mensch spielen"?

5. Effizienz versus Erklärbarkeit

Besonders effiziente Systeme können ihre guten Vorhersagen oft nicht begründen. Somit ist in jedem Anwendungsfall einzeln abzuschätzen, welchen Einfluss dies auf den Menschen hat. Kann zum Beispiel eine KI, die anhand einer großen Anzahl von Patientenakten trainiert wurde, einen Arzt ersetzen? Welche Entscheidung muss und soll individuell medizinisch begründet werden?

Bewährte Grundsätze der digitalen Unternehmensverantwortung

Welche digitalethische Strategie die richtige für eine Organisation ist, hängt von der individuellen Ausrichtung des Unternehmens ab. Dennoch haben sich in der Praxis branchen- und unternehmensübergreifend fünf Grundsätze für die Etablierung ethischer Standards bewährt[2]:

1. Sich der eigenen Verantwortung bewusst werden und Standards setzen

Unternehmen können das Potenzial der Digitalisierung nur dann voll ausschöpfen, wenn sie ihr Wertesystem mit integritätsfördernden Strukturen innerhalb des Hauses verknüpfen. Stimmen die strategische Ausrichtung und das unternehmerische Handeln überein, fördert dies die Glaubwürdigkeit des Unternehmens gegenüber den eigenen Mitarbeitern, aber auch gegenüber der Öffentlichkeit. Neben den in vielen Branchen existierenden hohen Standards (z. B. bei der Kreditvergabe oder der Behandlung von Menschen) kann dem Management ein Digital-Responsibility-Codex zur Orientierung dienen. Welche Werte dabei maßgeblich sind, bestimmt die Unternehmensleitung. In der Praxis haben sich diese sieben „Leitplanken" bewährt: Sicherheit und Qualität (wie Datenschutz und -sicherheit), Transparenz (Nachvollziehbarkeit), Privatheit (Achtung der Privatsphäre), Nutzen und Wohl (Nachhaltigkeit), Verantwortung und Nachvollziehbarkeit (Erklärbarkeit), Diskriminierungsfreiheit und Recht (Wahrung der Menschenrechte und Gesetze) sowie Partizipation (Teilhabe, Empowerment).

2. Parallelstrukturen vermeiden, auf Vorhandenes aufsetzen

Digitalethische Grundsätze können im Unternehmen nur dann erfolgreich verankert werden, wenn sie an bestehende betriebliche Strukturen und Prozesse anknüpfen. Damit dies gelingt, sollten digitalethische Werte in den bestehenden Managementsystemen, zum Beispiel im Risiko- und Compliance-Management und bei der Personalentwicklung, einen festen Platz erhalten. Das steigert auch die Akzeptanz in der Belegschaft. Dagegen sollten Unternehmen es in jedem Fall vermeiden, Parallelstrukturen aufzubauen. So gewinnen sie langfristig das Vertrauen ihrer Stakeholder. Um diese Integration zu unterstützen, hat PwC das Tool Integrity Driven Performance (IDP) entwickelt, das sich konsequent am Wert der Integrität orientiert.

3. Kompetenz aufbauen – bei der Belegschaft wie auf der Leitungsebene

Unternehmen bezeichnen in der PwC-Studie die fehlende Kompetenz und das mangelnde Bewusstsein innerhalb der Mitarbeiterschaft als die größte Hürde auf dem Weg zur digitaler Ethik. In der Gesundheitsbranche ist sicherzustellen, dass die hohen ethischen Standards, die im täglichen Umgang mit den Patienten gelten, von den Mitarbeitern auch im Umgang mit Technologien angewendet werden. Daher ist es wichtig, die digitalethische Kompetenz in der Belegschaft aufzubauen – auch um Unsicherheiten und Fehlverhalten vorzubeugen. Schon bei der Einstellung neuer Mitarbeiter sollten Unternehmen darauf achten, dass diese die Werte der Organisation teilen und zur Unternehmenskultur passen. Die schnelle technologische Entwicklung erfordert es zudem, dass Mitarbeiter kontinuierlich weitergebildet werden, etwa in Awareness-Workshops oder mithilfe neuer Lernformen auf der Basis von Apps. Eine wichtige Vorbildfunktion kommt der Leitungsebene bei der Ausbildung digitalethischer Kompetenz zu. Führungskräfte sind es auch, die dafür Sorge tragen müssen, dass Werte und Handeln übereinstimmen.

4. Geschäftsprozesse unternehmensübergreifend betrachten

Die Stärkung der Mitarbeiterkompetenz ist ein wichtiger Baustein der digitalethischen Strategie eines Unternehmens. Doch im Zeitalter der Digitalisierung mit stark vernetzten Strukturen reicht diese Maßnahme allein nicht mehr aus, da

die Grenzen zwischen dem eigenen Unternehmen, anderen Marktteilnehmern und externen Dienstleistern, insbesondere bei Plattformökonomien, verschwimmen. Daher sollten alle Teilnehmer einer Wertschöpfungskette einen gemeinsamen Werte- und Verhaltenskodex in ihren Geschäftsprozessen verankern und Transparenz herstellen, etwa um die faire Behandlung und Bezahlung von Mitarbeitern sicherzustellen. Allerdings verfügen bislang nur wenige Unternehmen über Erfahrung in diesem Bereich. Hier ist bei vielen ein Umdenken erforderlich. Mehr Kooperation sowie Schulungen können Abhilfe schaffen und die notwendige Transparenz bei allen Stakeholdern ermöglichen.

5. Ethische Standards bei der Produktentwicklung berücksichtigen

Das Tempo der Digitalisierung zieht an und die Produktentwicklungsprozesse werden zunehmend agil gestaltet. Dies erschwert die Zugrundelegung ethischer Werte. Umso wichtiger ist es, ethische Standards bereits bei der Planung und Entwicklung neuer Technologien zu berücksichtigen. Das gelingt, indem klare Verantwortlichkeiten für die Mitarbeiter festgelegt werden, die den Produktentwicklungsprozess begleiten. Eine weitere Möglichkeit stellen Zertifizierungen dar, durch die sich Unternehmen langfristig absichern und vom Wettbewerb abheben können und mit denen sie das Vertrauen in ihre Dienstleistungen und Produkte stärken.

Wie in der analogen Welt gilt auch für das digitale Zeitalter, dass sich jeder seiner Verantwortung bewusst sein muss und dass man nur durch Transparenz und Nachvollziehbarkeit von Entscheidungen Vertrauen schaffen kann.

CDR und Daten – die Verantwortung des Datenschutzbeauftragten wächst

Verantwortung endet nicht an der Unternehmensgrenze. Durch die zunehmende Vernetzung von Unternehmen, die mit den neuen Technologien einhergeht, werden vertrauensvolle Geschäftsbeziehungen immer wichtiger, nicht zuletzt, um das eigene Risiko zu minimieren. Mit einer ganzheitlichen CDR-Strategie können sich Unternehmen als vertrauenswürdiger Partner positionieren. Es gilt ein Netzwerk aus vertrauenswürdigen Partnern aufzubauen und in Bezug auf die Datenlieferkette Nachvollziehbarkeit und Transparenz sicherzustellen sowie Informationen über die eigenen Unternehmensgrenzen hinaus zu generieren. Sowohl in der Wirtschaft als auch in der Politik gibt es Bestrebungen zur Erarbeitung eines einheitlichen Standards. Dieser würde den Unternehmen Klarheit über den Sollzustand eines verantwortungsvollen Umgangs mit Daten verschaffen und durch entsprechende Testate Sicherheit bieten. Perspektivisch wäre dann eine noch intensivere Zusammenarbeit mit Partnern aus dem Netzwerk denkbar, die sich auf dieselben Werte geeinigt haben und nach dem gleichen Standard attestiert sind.

Auch auf gesetzlicher Ebene wurde Handlungsbedarf erkannt. Im Rahmen einer Konferenz der Datenschutzbehörden des Bundes und der Länder im November 2019 wurde ein Erfahrungsbericht vorgestellt, der nahelegt, dass die DSGVO an einigen Stellen überarbeitet werden sollte. Die Verbesserungsvorschläge betreffen hauptsächlich die Themen Profiling, Privacy by Design und Bürokratie. Zum einen geht es darum, wie das Gesetz an manchen Stellen klarer formuliert werden könnte, um Auslegungsfragen zu klären. Zum anderen werden konkrete Vorschläge für neue oder veränderte Regelungen gemacht, etwa zur Reduzierung des bürokratischen Aufwands oder zur Verschärfung bisheriger Artikel der DSGVO. Dem Datenschutzbeauftragen obliegt es hier stets auf dem Laufenden zu bleiben und entsprechende Änderungen im Unternehmen umzusetzen.

Neues Rollenkonzept für Datenschutzbeauftragte und Chief Data Officer

Die Ausrichtung unternehmerischen Handelns an digitalethischen Werten muss an fest definierte Rollen und Prozesse gekoppelt werden. Anderenfalls lässt sich diese Aufgabe nicht effektiv bewältigen. Zudem haben Mitarbeiter und andere Stakeholder dadurch klare Ansprechpartner für ihre Fragen.

Die konkrete Umsetzung lässt sich vielfältig gestalten. So können zum Beispiel neue Rollen definiert werden, wie es das US-amerikanische Softwareunternehmen Salesforce mit der Einführung des Chief Ethical and Humane Use Officer gemacht hat. Dessen Aufgabe ist es, die ethische Nutzung von Technologien im Unternehmen, bei der der Mensch im Mittelpunkt steht, sicherzustellen. Interdisziplinär zusammengestellte Digital Ethics Boards wären eine weitere Möglichkeit, um die Digitalisierung im Unternehmen ethisch verantwortungsvoll umzusetzen. Nicht selten werden auch Externe in diese Boards aufgenommen, um neutralen Sichtweisen oder Stakeholderinteressen Raum zu geben.

Digitale Ethik und Verantwortung lassen sich aber auch in bereits existierende Rollen integrieren. Da im Unternehmen ein Kulturwandel stattfinden muss und CDR in der Unternehmens-DNA verankert werden soll, empfiehlt es sich sogar, auf vorhandene Rollenkonzepte aufzubauen, indem diese um neue Aspekte und Aufgabenfelder erweitert werden. Dies kann die Akzeptanz seitens der Mitarbeiter deutlich erhöhen. So kann der Datenschutzbeauftragte über seine Aufgaben, wie sie im Artikel 39 der DSGVO definiert sind, hinaus eine wesentliche Rolle spielen. Als Interner oder Externer analysiert und kontrolliert er das Datenschutzniveau des Unternehmens. Auf der Basis seiner DSGVO-Expertise ▸

berät er die Verantwortlichen zu Auslegungsfragen und Verbesserungsmöglichkeiten und ist darüber hinaus Ansprechpartner der Geschäftsführung. Damit ist er prädestiniert, die Umsetzung eines verantwortungsvollen Umgangs mit Daten im Unternehmen zu fördern und die jeweiligen Abteilungsvertreter bei der Ausgestaltung zu beraten.

Zusätzlich empfiehlt sich die Einführung eines Chief Data Officer (CDO). Dieser trägt die Verantwortung für die Datenstrategie und das Datenmanagement, vor allem hinsichtlich der neuen digitalen Services und Produkte. Der CDO sollte mit dem Datenschutzbeauftragten eng zusammenarbeiten, damit ein konsistentes Konzept für den Umgang mit Daten im Unternehmen erarbeitet werden kann. Der CDO müsste zunächst die Datenethikprinzipien für einen Digital-Responsibility-Codex definieren – in Einklang mit den Werten und Best Practices des Unternehmens. Laut der oben genannten PwC-Studie haben bereits über 60 Prozent der befragten Unternehmen solche digitalethischen Leitlinien als Bestandteil ihrer Unternehmenskultur definiert.

Darin werden unter anderem die Verantwortlichkeiten auf den verschiedenen Unternehmensebenen und Prozesse zur kontinuierlichen Bewertung gesellschaftlicher Anforderungen festgelegt sowie Anforderungen an die Mitarbeiterweiterbildung im digitalen Bereich definiert. Um sowohl das Bewusstsein für digitalethische Anforderungen im Unternehmen als auch die gesellschaftliche Akzeptanz neuer Technologien zu fördern, empfiehlt es sich, den Kodex beziehungsweise die Leitlinien allen internen und externen Interessengruppen zugänglich zu machen. Aus den Leitlinien sind dann geeignete Maßnahmen abzuleiten, die wiederum mit Kontrollen versehen werden müssen. Die Maßnahmenumsetzung sollte jederzeit durch Externe überprüfbar sein. Des Weiteren obliegt es dem CDO sämtliche beteiligte Abteilungen – also nicht nur die strategischen, sondern auch die Produktentwicklung – mit den Werkzeugen und Methoden auszustatten, die für die Wahrnehmung der digitalen Unternehmensverantwortung notwendig sind. Nur so kann er den nachhaltigen Erfolg der Maßnahmen sicherstellen.[3]

Fazit

Damit Digitalisierungsvorhaben von Unternehmen erfolgreich umgesetzt werden können, braucht es eine breite Akzeptanz der neuen Technologien und datenbasierten Geschäftsmodelle in der Gesellschaft. Die Einhaltung der DSGVO allein reicht hierfür nicht aus. Das übergeordnete Ziel von Unternehmen muss es daher sein, frühzeitig für Transparenz über den Umgang mit Daten zu sorgen und das diesbezügliche Vertrauen bei Mitarbeitern, Kunden, Geschäftspartnern, Behörden und in der Öffentlichkeit zu stärken. Erreichen lässt sich das Ziel durch eine werteorientierte, verantwortungsvolle digitale Transformation. Dazu ist es erforderlich eine digitale Ethik in Einklang mit der DSGVO und den Unternehmenswerten zu erarbeiten und in der Unternehmenskultur, aber auch in der gesamten Wertschöpfungskette zu verankern. Die sich daraus ergebenen Aufgaben und Verantwortlichkeiten sollten den bestehenden oder neu zu schaffenden Rollen, etwa dem Datenschutzbeauftragten und dem CDO, fest zugeordnet werden. Darüber hinaus ist es zielführend, dass digitalethische Aspekte von Beginn an in die Ausarbeitung neuer Gesetze und Regularien mit einfließen. So erhalten die Unternehmen einen digitalethischen Kompass, der ihnen auch in diesem Bereich der digitalen Transformation sicher den Weg weist.

Literaturverzeichnis

[1]Horst, D.; Vehlow M.; Pauer, A. (2018): Digitalisierung verantwortungsvoll gestalten, abgerufen am 16.06.2020 unter: https://www.pwc.de/de/nachhaltigkeit/digitalisierung-verantwortungsvoll-gestalten.html

[2]Paffen, R.; Hanauer, D.; Esche, S.; Reese, H.; Pauer, A.; Vehlow, M.; Dzombeta, S. (2020): Digitale Ethik. Orientierung, Werte und Haltung für eine digitale Welt, abgerufen am 16.06.2020 unter:www.pwc.de/de/managementberatung/risk/digitale-ethik.html

[3]Pauer, A.; Stoppelkamp, A.; Becke, S. (2020): Die Rolle von Aufsichtsrat und Chief Digital Officer, in: Unternehmensverantwortung im digitalen Wandel - Ein Debattenbeitrag zu Corporate Digital Responsibility, Bertelsmann Stiftung, Wittenberg-Zentrum für Globale Ethik (Hrsg.), ISBN 978-3-86793-915-7

Über die Autoren

Angelika Pauer
Senior Managerin, Corporate Digital Responsibility & Digital Ethics Services, PwC GmbH

▶ angelika.pauer@pwc.com

Saskia Becke
Associate, Corporate Digital Responsibility & Digital Ethics Services, PwC GmbH

▶ saskia.becke@pwc.com

Daniela Hanauer
Partnerin, Integrity Driven Performance & Digital Ethics, PwC GmbH

▶ daniela.hanauer@pwc.com

Paul Czech
Senior Associate, Trust in AI & Digital Ethics, PwC GmbH

▶ paul.czech@pwc.com

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.

ZWEI JAHRE DSGVO – DIE BILANZ DER EUROPÄISCHEN KOMMISSION

Dr. Tilman Dralle

I. Einleitung

Zwei Jahre nach dem 25. Mai 2018 hat die Europäische Kommission am 24. Juni 2020 ihren ersten Bericht über die „Bewertung und Überprüfung" der Datenschutz-Grundverordnung (DSGVO) vorgelegt.[1] Nach Ansicht der Kommission hat die DSGVO ihre Ziele, zwei Jahre nach Geltungsbeginn, erfolgreich erreicht. Das Recht jedes Einzelnen auf Datenschutz sei gestärkt und der freie Verkehr personenbezogener Daten innerhalb der EU verbessert worden.[2] Gleichzeitig identifiziert die Kommission einige Bereiche mit Verbesserungspotenzial und lehnt es insofern ab abschließende Schlussfolgerungen zu formulieren.[3] Dieser Beitrag gibt einen schlaglichtartigen Überblick über einige der wichtigsten Themenfelder der Kommissionsbilanz und ergänzt ihn, wo passend, mit Kontext und Kommentar.

II. DSGVO: Die Bilanz

Ausstattung der Datenschutz-Aufsichtsbehörden

Als Erfolg vermeldet die Kommission, dass den meisten Datenschutz-Aufsichtsbehörden seit 2016 mehr Personal und Budget zur Verfügung steht. So ist die personelle Ausstattung zwischen 2016 und 2019 um 42%, das gesamte Budget sogar um 49% gestiegen.[4] Gleichzeitig sind große Unterschiede zwischen den Mitgliedstaaten zu verzeichnen. Während die Behörden in Irland, den Niederlanden, Island, Luxemburg und Finnland von erheblichem Personalzuwachs profitierten (bis zu 169% in Irland), sank die Anzahl der MitarbeiterInnen in Griechenland, Bulgarien, Estland, Lettland und Litauen (bis zu -15% in Griechenland).[5] Die deutschen Datenschutzbehörden haben mit 888 MitarbeiterInnen (2019) die höchste Personalausstattung, gefolgt von Polen mit 238. Relativ zur Bevölkerung gesehen weisen allerdings neun Datenschutz-Aufsichtsbehörden innerhalb der EU/EEA eine bessere Personalsituation auf.[6] Dieselbe Sicht ergibt sich auch beim Budget. Für die Datenschutz-Aufsichtsbehörden in Irland und Luxemburg sieht die Kommission einen „spezifischen Ressourcenbedarf" aufgrund ihrer Rolle als federführende Aufsichtsbehörden für die Umsetzung der DSGVO gegenüber großen, internationalen Technologieunternehmen, die schwerpunktmäßig in diesen beiden EU-Mitgliedstaaten ansässig sind.[7]

Maßnahmen zur Durchsetzung

Nach Ansicht der Kommission haben die Datenschutz-Aufsichtsbehörden die ihnen zur Verfügung stehenden Abhilfebefugnisse ausgewogen genutzt. In Deutschland wurde das höchste Bußgeld gegen den Berliner Immobilienkonzern Deutsche Wohnen SE verhängt: 14,5 Millionen Euro. Das im europäischen Vergleich bislang höchste Bußgeld – 50 Millionen Euro – wurde von der französischen Commission nationale de l'informatique et des libertés (CNIL) im Januar 2019 gegen Google LLC ausgesprochen.[8] Die Bußgeldentscheidung der CNIL wurde vom französischen Conseil d'État im Juni 2020 weitgehend bestätigt.[9]

[1] Europäische Kommission, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM(2020) 264 final, 24.6.2020 (im Folgenden zitiert als „Communication"); Europäische Kommission, Commission staff working document, SWD(2020) 115 final, 24.6.2020 (im Folgenden zitiert als „Staff Working Document"). Die Berichtspflicht ergibt sich aus Art. 97 DSGVO.

[2] Fn. 1, Communication, 4.

[3] Ibid., 4.

[4] Fn. 1, Staff Working Document, 12.

[5] Ibid.

[6] Ibid., 52.

[7] Ibid., 13-14; Fn. 1, Communication, 6.

[8] Siehe hierzu Dralle, BvD-News 1/2019, 38.

[9] Siehe <https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil>, abgerufen am 28.6.2020.

Als unzureichend moniert die Europäische Kommission die Durchsetzungsbemühungen gegenüber ausländischen datenverarbeitenden Unternehmen, die aufgrund des erweiterten räumlichen Anwendungsbereichs[10] ebenfalls an die Bestimmungen der DSGVO gebunden sind. Das Fehlen einer Niederlassung in der EU dürfe nicht als Freifahrtschein verstanden werden.[11] Ein erster Ansatzpunkt für die Durchsetzung der datenschutzrechtlichen Vorgaben könne die Pflicht sein in der Union einen Vertreter gemäß Art. 27 DSGVO zu benennen.

Beratung und Leitlinien

Der Europäische Datenschutzausschuss (EDPB) hat bis Ende 2019 insgesamt 67 Dokumente beschlossen, darunter 10 neue Leitlinien sowie 43 Stellungnahmen, insbesondere zu Listen von Verarbeitungsvorgängen, für die (k)eine Datenschutz-Folgenabschätzung durchzuführen ist.[12] Weitere Leitlinien sind in Arbeit. Hinsichtlich der Beratung durch nationale Datenschutz-Behörden nahm die Europäische Kommission in ihren Bericht auch Kritik von Interessenvertretern auf. So gebe es beispielsweise zwischen den Aufsichtsbehörden der EU-Mitgliedstaaten unterschiedliche Auffassungen zu Cookies, der Auslegung berechtigter Interessen, der Mitteilungspflicht bei Datenschutzverletzungen sowie zur Datenschutz-Folgenabschätzung.[13] Selbst zwischen den Aufsichtsbehörden eines Mitgliedstaates fehle es teilweise an einem einheitlichen Vorgehen, so z.B. in Deutschland hinsichtlich der Definitionen „Verantwortlicher" und „Auftragsverarbeiter".[14]

Die von Interessenvertretern kritisierten Unterschiede bei der Auslegung und Anwendung der Bestimmungen zum Umgang mit Datenschutzverletzungen können auch mit Zahlen aus dem Kommissionsbericht unterlegt werden. So variieren die gemeldeten „data breaches", berechnet auf eine Million Einwohner, zwischen 14 (Bulgarien) und 2150 (Niederlande).[15]

Internationaler Datentransfer

Der im Januar 2019 verabschiedete Angemessenheitsbeschluss für Japan wird von der Europäischen Kommission als Meilenstein und „nützlicher Präzedenzfall" für die Zukunft gewürdigt. Es ist der erste Angemessenheitsbeschluss nach Geltungsbeginn der DSGVO. Darüber hinaus sind die Verhandlungen mit Südkorea in einem fortgeschrittenen Stadium, und auch für Großbritannien wird eine Angemessenheitsprüfung durchgeführt. Mit anderen wichtigen Partnern in Asien und Lateinamerika laufen entsprechende Sondierungsgespräche.

Gleichzeitig geht die Europäische Kommission davon aus, dass das vor dem Europäischen Gerichtshof (EuGH) anhängige Verfahren Schrems II (C-311/18) Auswirkungen auf Angemessenheitsbeschlüsse nach Art. 45 DSGVO haben könnte.[16] Denn auch wenn sich Schrems II schwerpunktmäßig auf den Übertragungskanal der Standardvertragsklauseln bezieht, so könnte das für den 16. Juli 2020 erwartete Urteil direkte oder indirekte Effekte sowohl für den Angemessenheitsbeschluss „EU-U.S. Privacy Shield" als auch für den Angemessenheitsstandard als solchen zeitigen.

Als zweiten wichtigen Baustein für internationale Datentransfers überarbeitet die Europäische Kommission derzeit den am häufigsten genutzten Übertragungskanal: Die Standardvertragsklauseln (SCC).[17] Insbesondere sollen bei diesem „Update" die durch die DSGVO eingeführten Neuerungen wie z.B. die erweiterten Auftragsverarbeiterpflichten sowie die Informationspflichten berücksichtigt werden. Außerdem werden die überarbeiteten SCC nach den Plänen der Kommission bislang unberücksichtigte Übermittlungsszenarien umfassen, wie die Übermittlung von Daten von einem EU-Auftragsverarbeiter zu einem Unterauftragsverarbeiter in einem Drittland sowie Situationen, in denen der Verantwortliche nicht in der EU ansässig ist. Ferner prüft die Kommission die Möglichkeit der Unterzeichnung von SCC durch mehrere Parteien oder des Beitritts zur Vertragslaufzeit.[18]

Allerdings könnte das kurz bevorstehende EuGH-Urteil im Schrems II-Verfahren erhebliche Auswirkungen auf die Ausgestaltung der SCC haben, auch wenn Generalanwalt Henrik Saugmandsgaard Øe in seinen Schlussanträgen die Gültigkeit der Controller-to-Processor-SCC[19] bestätigte.[20] Daher erwägt die Kommission, die SCC hinsichtlich des Zugriffs ausländischer öffentlicher Stellen auf mithilfe der SCC übertragene personenbezogene Daten, bspw. zu Zwecken der nationalen Sicherheit, zu ▶

[10] Art. 3 Abs. 2 DSGVO.

[11] Fn. 1, Communication, 12; Fn. 1, Staff Working Document, 31.

[12] Fn. 1, Communication, 6.

[13] Fn. 1, Staff Working Document, 10.

[14] Ibid., 10.

[15] Eigene Berechnung basierend auf: Fn. 1, Staff Working Document, 11; Europäischer Datenschutzausschuss, Contribution of the EDPB to the evaluation of the GDPR under Article 97, 28.2.2020, 35. Deutschland hat mit 45561 Fällen absolut gesehen die höchste Anzahl an Datenschutzverletzungen. Relativ gesehen sind es 548 Meldungen auf 1 Million Einwohner.

[16] Zu den Ende 2019 vorgelegten Schlussanträgen des EuGH-Generalanwalts Saugmandsgaard Øe siehe Dralle, BvD-News 1/2020, 39.

[17] Art. 46 Abs. 2 Buchst. c DSGVO. Die DSGVO nutzt die Terminologie „Standarddatenschutzklauseln".

[18] Fn. 1, Staff Working Document, 37.

[19] Beschluss 2010/87/EU.

[20] Fn. 16, 39.

präzisieren.[21] Ziel sollte es sein die SCC so anzupassen, dass insbesondere kleine und mittelständische Unternehmen nicht dazu gezwungen sind für jeden Drittstaatentransfer eine umfassende Verhältnismäßigkeitsprüfung der jeweiligen ausländischen Rechtsordnung ohne Hilfestellung der Datenschutz-Aufsichtsbehörde durchzuführen.

Last but not least fordert die Kommission eine Verschlankung des Genehmigungsprozesses für Binding Corporate Rules (BCRs), den Abschluss der Arbeiten des EDPB an Kriterien für die Genehmigung von Zertifizierungsmechanismen als Instrument für internationale Datentransfers sowie eine Präzisierung des Verhältnisses zwischen Art. 3 DSGVO zur Anwendbarkeit der DSGVO auch in Drittstaaten und den Regeln zu Drittstaatentransfers in Kapitel V DSGVO.[22]

Fragmentierung durch nationale Gesetzgebung

Auch im Hinblick auf die Harmonisierungswirkung der DSGVO zieht die Kommission Bilanz. Sie identifiziert eine Reihe von Missständen, die aus ihrer Sicht zu einer Fragmentierung der Rechtsordnung führen. So haben die EU-Mitgliedstaaten die von der DSGVO eröffneten Spielräume bei der Festlegung der Altersgrenze für eine wirksame Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft vollumfänglich ausgenutzt: Von 13 bis 16 Jahren sind alle Ausprägungen vertreten. Dies konterkariere die Schaffung eines gleichen Schutzniveaus sowie den freien Fluss personenbezogener Daten in der EU, so die Kommission.[23]

Auch weitgehende Beschränkungen von Betroffenenrechten stehen in der Kritik. Die entsprechenden europarechtlichen Anforderungen in Art. 23 DSGVO würden häufig nicht angemessen beachtet. Eine mitgliedstaatliche Beschränkung von Betroffenenrechten, die nach Ansicht der Kommission eindeutig über den Anwendungsbereich der Öffnungsklausel hinausgeht, ist die Einschränkung des Rechts auf Auskunft bei einem „unverhältnismäßigen Aufwand" aufseiten des Verantwortlichen.[24] Das deutsche Bundesdatenschutzgesetz (BDSG) sieht eine solche Beschränkung in § 34 Abs. 1 („Auskunftsrecht der betroffenen Person") vor. Damit scheinen sich die bereits zum Zeitpunkt der Verabschiedung des ersten DSAnpUG-EU geäußerten Zweifel an der europarechtlichen Zulässigkeit der Vorschrift zu erhärten.

Des Weiteren verweist der Kommissionsbericht auf nationalstaatliche Regelungen in Bereichen, die von der DSGVO abschließend geregelt werden und einer Beschränkung bzw. Spezifizierung auf Ebene der EU-Mitgliedstaaten daher nicht offenstehen. Dies treffe insbesondere auf Vorschriften zu, die Bedingungen für Verarbeitungen auf Grundlage eines berechtigten Interesses festlegen.[25] Denn für die Rechtsgrundlage der Interessenabwägung sieht Art. 6 Abs. 2 DSGVO nicht die Möglichkeit vor, nationale Erlaubnistatbestände zu schaffen. Mit § 4 BDSG („Videoüberwachung öffentlich zugänglicher Räume") besteht auch hier eine bundesdeutsche Regelung, die offensichtlich europarechtswidrig ist.[26]

Schließlich wird auch die (zulässige)[27] Erweiterung der Benennungspflicht eines Datenschutzbeauftragten in § 38 BDSG von der Europäischen Kommission als „zusätzliche Belastung" und Abkehr vom risikobasierten Ansatz der DSGVO kritisiert.[28]

Verbandsklagen

Laut Kommissionsbericht haben bislang nur wenige EU-Mitgliedstaaten die in Art. 80 Abs. 2 DSGVO vorgesehene Möglichkeit genutzt, bei Verletzung konkreter Rechte einzelner betroffener Personen bestimmten Einrichtungen, Organisationen und Vereinigungen das Recht einzuräumen, Klage- und Beschwerderechte auch ohne Mandat auszuüben. In diesem Zusammenhang verweist die Europäischen Kommission auf ihren bereits 2018 vorgelegten Vorschlag für eine Richtlinie über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher,[29] die sich auch auf Verstöße gegen die DSGVO erstrecken soll. Der Kommissionsvorschlag sieht vor, dass qualifizierte Einrichtungen Unterlassungsklagen grundsätzlich auch ohne Mandatierung erheben dürfen. Darüber hinaus müsste für eine solche Verbandsklage nicht nachgewiesen werden, dass Verbraucher einen tatsächlichen Verlust oder Schaden erlitten haben.[30] Der Richtlinienvorschlag, zu dem Ende Juni 2020 eine politische Einigung erzielt wurde, geht insofern in zweifacher Hinsicht über Art. 80 Abs. 2 DSGVO hinaus und würde damit auch der Debatte über die unionsrechtliche Zulässigkeit der entsprechenden deutschen Regelungen im UWG und UKlaG ein Ende bereiten, die mit dem Ende Mai 2020 ergangenen Vorabentscheidungsersuchen des Bundesgerichtshofs in Sachen „VZBV gegen Facebook" ihren vorläufigen Höhepunkt erreicht hat.[31]

[21] Fn. 1, Staff Working Document, 37.

[22] Ibid., 31, 38-39.

[23] Ibid., 17.

[24] Ibid., 18-19.

[25] Ibid., 15-16.

[26] So schon Piltz, BDSG – Praxiskommentar für die Wirtschaft, 2018, 39ff. Siehe auch Dralle, BvD-News 3/2019, 41.

[27] Siehe Art. 37 Abs. 4 DSGVO.

[28] Fn. 1, Staff Working Document, 19.

[29] COM(2018) 184 final, 11.4.2018.

[30] Ibid., Art. 5.

Kleine und mittelständische Unternehmen

Die Europäische Kommission erkennt die besonderen Herausforderungen an, die sich aus der Umsetzung der DSGVO insbesondere für kleine und mittelständische Unternehmen (KMU) ergeben. Gleichzeitig betont die Kommission, dass Ausnahmen auf Grundlage der Größe eines datenverarbeitenden Unternehmens „nicht angemessen" wären, da von der Größe nicht auf die Risiken einer Datenverarbeitung für betroffene Personen geschlossen werden könne. Geringfügige und risikoarme Verarbeitungen dürften nicht genauso behandelt werden wie hochrisikoreiche und häufige Verarbeitungen – unabhängig von der Größe des Unternehmens, das sie durchführt.[32] Hingegen würdigt die Kommission auf KMU zugeschnittene Unterstützungsleistungen wie spezielle Publikationen, Seminare, Handbücher, Hotlines und Vorlagen. Eine Hintertür lässt sich die Kommission dann allerdings doch offen. Man werde prüfen, ob eine gezielte Änderung von Art. 30 Abs. 5 DSGVO möglicherweise zweckdienlich sein könnte.[33] Die von den deutschen Aufsichtsbehörden für den Bereich der Informationspflichten angeregte Ausnahme für KMUs bleibt unberücksichtigt.[34]

Änderungen der DSGVO

Den von wissenschaftlicher Seite sowie von Wirtschafts- und Verbraucherschutzverbänden vorgetragenen Forderungen nach einer Überarbeitung der DSGVO[35] erteilt der Kommissionsbericht – zumindest implizit – eine klare Absage. Nur im Bereich des Art. 30 Abs. 5 DSGVO (siehe soeben) sowie bei der Harmonisierung der Altersgrenze für wirksame Einwilligungen durch Kinder bei Diensten der Informationsgesellschaft gibt sich die Europäische Kommission einen „Prüfauftrag".[36] Im Übrigen sei die DSGVO „zukunftsfest". Mit ihren bewährten Prinzipien sei fallspezifisch zu klären, wie aktuellen Herausforderungen wie beispielsweise dem Einsatz neuer Technologien (Künstliche Intelligenz, Blockchain, Internet of Things, Gesichtserkennung, Quantenrechner) begegnet werden kann.[37]

Über den Autor

Dr. iur. Tilman M. Dralle, LL.M. (Nottingham)
Senior Data Governance, Privacy & Compliance Manager, 1&1 IONOS SE, Lehrbeauftragter an der Juristischen Fakultät der TU Dresden

[32] Siehe BGH, Beschluss v. 28. Mai 2020, I ZR 186/17. Zur grundlegenden Frage der Sperrwirkung der DSGVO siehe bereits Dralle, BvD-News 3/2018, 10.

[32] Fn. 1, Staff Working Document, 23.

[33] Fn. 1, Communication, 15.

[34] Siehe Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, November 2019, 7-8.

[35] Um nur ein Beispiel zu nennen: Roßnagel / Geminn, Evaluation der Datenschutz-Grundverordnung aus Verbrauchersicht – Gutachten im Auftrag des Verbraucherzentrale Bundesverbands e.V. (vzbv), 26.11.2019.

[36] Fn. 1, Communication, 15.

[37] Fn. 1, Staff Working Document, 28.

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

SICHERHEIT DER VERARBEITUNG

Modell zur Planung, Umsetzung und Überprüfung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO

Dr. Gunther Schlöffel

1. Einleitung

Im Oktober 2019 verhängte der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg ein Bußgeld in Höhe von 100.000 € gegen ein mittelständisches Lebensmittelhandwerksunternehmen, da es Unterlagen von Bewerbern nur unzureichend gegen unberechtigten Zugriff gesichert hatte und diese in der Folge für prinzipiell jeden über das Internet einsehbar waren.

Dieses Beispiel zeigt einen der ersten Fälle in Deutschland, bei denen eine Aufsichtsbehörde einen Verstoß gegen den Grundsatz der Sicherheit der Verarbeitung sowie gegen die Pflicht, durch technische und organisatorische Maßnahmen ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten sicherzustellen, mit einem derart hohen Bußgeld geahndet hat.

Der im Beispiel dargelegte Rechtsverstoß scheint eindeutig, denn hier führte das faktische Fehlen von technischen Maßnahmen zu dem ersichtlich nicht akzeptablen Ergebnis der Preisgabe von schützenswerten Daten im Internet.

Hat ein Verantwortlicher den Anspruch, nicht nur technisch und organisatorisch ein nicht zu beanstandendes Sicherheitsniveau herzustellen, sondern auch alle formalen Anforderungen der DSGVO und des BDSG bezüglich der Planung, Umsetzung und Überprüfung von technischen und organisatorischen Maßnahmen zu erfüllen, so findet er Vorgaben mit direktem Bezug hierzu in nicht weniger als vier Artikeln und sechs Erwägungsgründen (ErwG) der DSGVO, ergänzt durch drei Paragraphen des BDSG. Der Gestaltung des § 9 BDSG a. F. und seiner Anlage gegenübergestellt, zeigt sich das neue Recht komplexer, aufwändiger und mit mehr Notwendigkeit zur Interpretation und Auslegung.

Gleich an mehreren Stellen verweisen die DSGVO und das BDSG darauf, dass technische und organisatorische Maßnahmen insbesondere unter Berücksichtigung des Risikos zu treffen sind, welches durch die konkrete Verarbeitungstätigkeit für die Personen entsteht, deren Daten verarbeitet werden. Damit ist klargestellt, dass allein das Aufzählen umgesetzter Maßnahmen, wie es nach der alten Rechtslage möglich war, die Forderungen der DSGVO und des BDSG nicht erfüllen kann.

Die gestiegenen Anforderungen zusammen mit ihrer Auslegungsbedürftigkeit und dem Mangel an eindeutigen Vorgaben führen dazu, dass diese mit einem angemessenen Aufwand scheinbar kaum zu erfüllen sind. Neben der tatsächlichen Planung, Umsetzung und Überprüfung von Maßnahmen muss eine spezifische Risikoidentifikation und -bewertung durchgeführt sowie die entsprechende Dokumentation etabliert werden. Im Ergebnis fallen Verantwortliche nicht selten auf das Aufzählen der Maßnahmen zurück oder bleiben in ihrer Risikobewertung zu generisch, sodass diese den ihr zugedachten Mehrwert verfehlt.

Dieser Artikel betrachtet zunächst die mit der Planung, Umsetzung und Überprüfung technischer und organisatorischer Maßnahmen verbundenen gesetzlichen Anforderungen der DSGVO und des BDSG. Hernach interpretiert er diese im Kontext der geforderten Risikobewertung, um hierauf aufbauend ein Modell vorzuschlagen, welches die Anforderungen der DSGVO und des BDSG umsetzt, sich mit einem vertretbaren Aufwand einführen und betreiben lässt und sich in der Praxis bereits bewährt hat. Zwar ist die Umsetzung des Modells aufwändiger als das Führen von TOM-Listen, sein risikobasierter Ansatz zeigt in der Praxis aber tatsächlich einen Mehrwert bei der Planung geeigneter Schutzmaßnahmen.

2. Anforderungen

Anforderungen mit direktem Bezug zur Planung, Umsetzung und Überprüfung von technischen und organisatorischen Maßnahmen für gewöhnliche Verarbeitungstätigkeiten finden sich in den Art. 5, 24, 25 und 32 DSGVO sowie in §§ 64, 71 BDSG ergänzt durch die ErwG 74-78, 83 DSGVO.

Während in Art. 5 DSGVO die Gewährleistung einer angemessenen Sicherheit als einer der Datenschutzgrundsätze festgeschrieben ist, stellt Art. 24 DSGVO klar, dass dem Ver-

antwortlichen obliegt, diesen Grundsatz umzusetzen und eine Umsetzung geeigneter Maßnahmen nachweisen zu können. Art. 25 DSGVO hebt den Stellenwert der technischen und organisatorischen Maßnahmen als Mittel zum Schutz der verarbeiteten Daten und zur Sicherstellung der Datenschutzgrundsätze hervor. Schließlich führt Art. 32 DSGVO den Begriff des dem Risiko angemessenen Schutzniveaus ein.

Die zentrale Anforderung, dass Planung, Umsetzung und Überprüfung von technischen und organisatorischen Maßnahmen unter der Berücksichtigung des Risikos, welches durch die Verarbeitung für die betroffene Person entsteht, zu erfolgen hat, findet sich in den Art. 24, 25 und 32 DSGVO sowie in § 64 BDSG.

Da die Gestaltung und der Inhalt des Art. 32 DSGVO i.V.m. § 64 BDSG einer konkreten Beschreibung der Anforderungen hinsichtlich der Planung, Umsetzung und Überprüfung technischer und organisatorischer Maßnahmen am nächsten kommt, werden die Bestandteile des Art. 32 Abs. 1 S. 1 in Abb. 1 dargestellt und nachfolgend auf ihre wesentliche Bedeutung hin untersucht. {Datenschutzkonferenz [Hrsg.], Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, 2018};

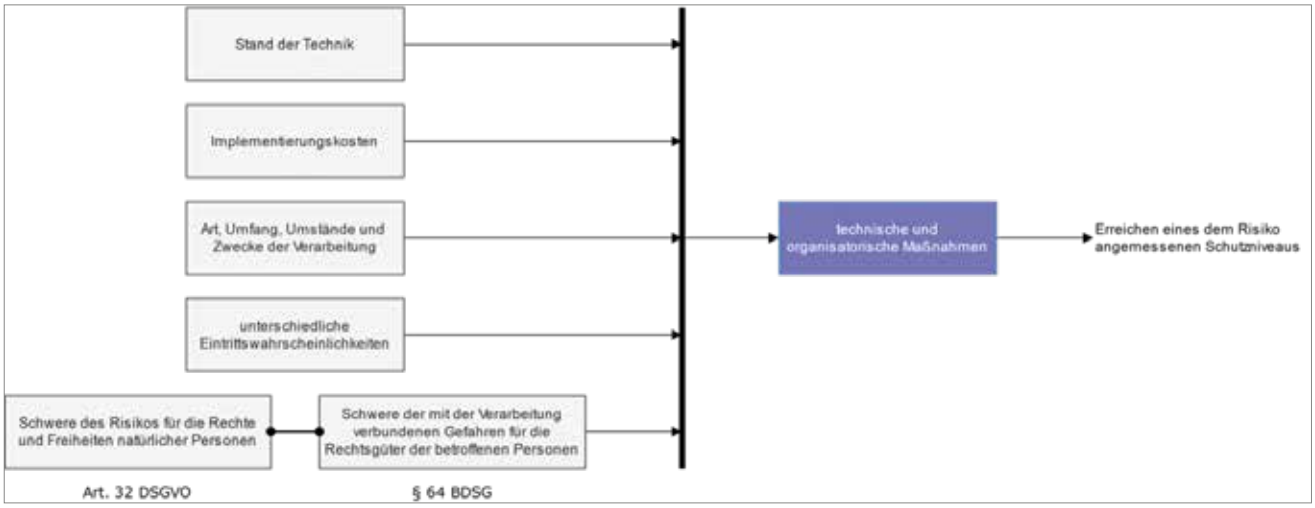


Abb. 1: Anforderungen der DSGVO und des BDSG für Planung und Umsetzung von technischen und organisatorischen Schutzmaßnahmen

Art. 32 Abs. 1 S. 1 DSGVO:

> *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten (...)"*

lässt dem Verantwortlichen die Möglichkeit Maßnahmen, deren Kosten nicht im Verhältnis zu ihrem Nutzen stehen, nicht umzusetzen, außer der Stand der Technik legt deren Umsetzung nahe. Mit den wesentlichen Aspekten zum Stand der Technik setzt sich eine Handreichung des TeleTrusT auseinander {Bundesverband IT-Sicherheit e.V. (TeleTrusT) [Hrsg.], Handreichung zum „Stand der Technik", 2019};

> *„(...) und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung (...)"*

fordert eine Verknüpfung der getroffenen Maßnahmen mit den einzelnen Verarbeitungstätigkeiten, so auch die Datenschutzkonferenz (DSK) in ihren Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO

> *„(...) sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (...)"*

fordert einen klassischen risikobasierten Ansatz mit der Besonderheit, solche Risiken zu betrachten, die den betroffenen Personen, deren Daten verarbeitet werden, durch die Verarbeitung entstehen;

> *„(...) treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, (...)"*

fordert Planung und Umsetzung von geeigneten Schutzmaßnahmen und i.V.m. Art. 32 Abs. 1 HS. 2 lit. d deren regelmäßige Überprüfung vom Verantwortlichen oder Auftragsverarbeiter;

> *„(...) um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;"*

fordert ein Vorgehen, welches das Risiko berücksichtigt und festzustellen erlaubt, dass ein angemessenes Schutzniveau erreicht ist;

3. Risikobewertung

Der Begriff der Risikobewertung findet sich in § 64 Abs. 3 S. 1 BDSG, welcher für den Fall einer automatisierten Verarbeitung die Durchführung einer Risikobewertung fordert. Jedoch kann die in Art. 32 DSGVO sowie in § 64 BDSG gestellte allgemeine Anforderung der Sicherstellung eines dem Risiko angemessenen Schutzniveaus prinzipiell nur dann sinnvoll erfüllt werden, wenn konkrete Risiken identifiziert und bewertet werden, die in einem tatsächlichen Zusammenhang mit der konkret durchgeführten Verarbeitungstätigkeit stehen.

Folglich ist anzunehmen, dass zur Erfüllung des Art. 32 DSGVO eine spezifische Risikobewertung ohne Ausnahme durchzuführen ist. Diese Ansicht vertritt im Fazit auch das von der Datenschutzkonferenz herausgegebene Kurzpapier Nr. 18 zum Thema Risiko {Datenschutzkonferenz [Hrsg.], Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, 2018}.

ErwG. 77 DSGVO führt an, dass Anleitungen zur Durchführung der Risikobewertung durch erlassene Leitlinien gegeben werden können. Noch scheinen solche Leitlinien allerdings nicht verfügbar zu sein. Ausgehend von allgemeinen Grundsätzen zur Durchführung einer Risikobewertung, wie man sie zum Beispiel in der DIN ISO 31000 {DIN Deutsches Institut für Normung e. V., DIN ISO 31000:2018-10, Risikomanagement - Leitlinien, 2018} oder in den BSI-Standards {Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 200-3, Risikoanalyse auf Basis von IT-Grundschutz} findet, besteht eine Risikobewertung im Kern aus einem Prozess zur Identifikation und Bewertung der Risiken, aus einer zu dem Prozess passenden Form der Dokumentation sowie aus einem Schema und zugehörigen Metriken, welche die Quantifizierung bzw. Kategorisierung von Schäden, Eintrittswahrscheinlichkeiten und Risiken ermöglichen.

Abb. 2 stellt ein generisches Schema einer DSGVO-konformen Risikobewertung dar, wie es sich aus den verschiedenen Anforderungen der DSGVO und des BDSG zu ergeben scheint.

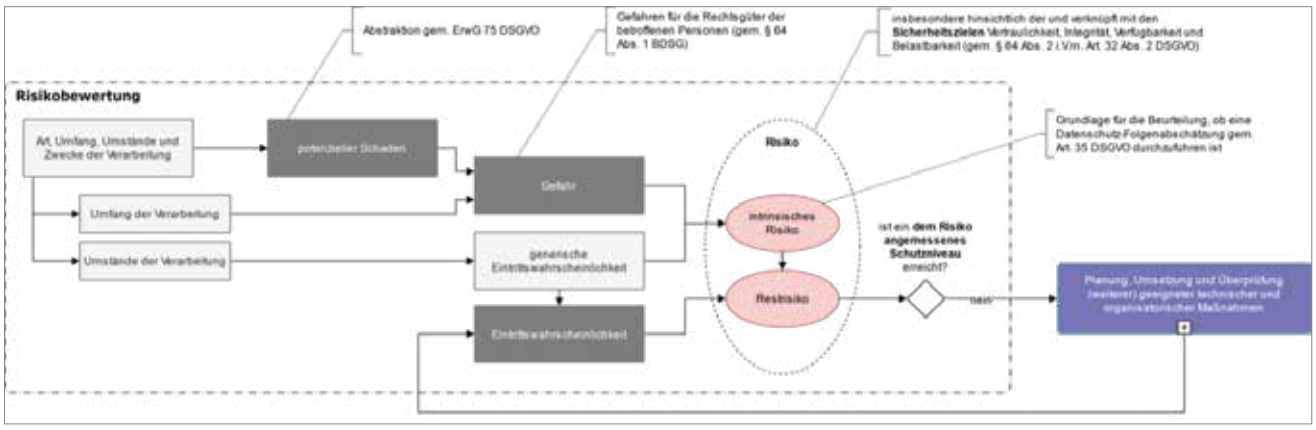


Abb. 2: Risikobewertung gemäß den Anforderungen von DSGVO und BDSG

3.1. Risiko

Während Art. 32 Abs. 1 DSGVO von den „Risiken für die Rechte und Freiheiten natürlicher Personen" spricht, benutzt § 64 Abs. 1 BDSG im gleichen Zusammenhang den Ausdruck der „mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen". Im Kontext einer Risikobewertung haben die Begriffe „Gefahr" und „Risiko" jedoch verschiedene Bedeutungen.

Ein Risiko wird allgemein als die Auswirkung von Unsicherheiten auf Ziele definiert. Während eine Gefahr als Risikoquelle ein Element ist welches alleine oder gemeinsam mit anderen Faktoren potenziell zu Risiken führt. Vereinfacht gesagt ergibt sich ein Risiko aus der Kombination eines mit einer Gefahr verknüpften potenziellen Schadens und der Wahrscheinlichkeit, dass sich dieser Schaden tatsächlich realisiert.

Zunächst scheint deshalb unklar, ob die Gefahren oder die Risiken im Zentrum der Bewertung nach der DSGVO und des BDSG stehen soll.

Aufschluss kann eine Betrachtung der Systematik der Art. 35 und 36 DSGVO geben. Auch Art. 35 DSGVO spricht von einem Risiko. Art. 36 DSGVO verdeutlicht je-

doch, dass das Ergebnis dieser Risikobewertung von den zu treffenden Maßnahmen nicht abhängen darf. Art. 35 DSGVO lässt folglich darauf schließen, dass es eine Bewertung des „Risikos" geben muss, in welches höchstens eine intrinsische oder allgemeine Eintrittswahrscheinlichkeit Eingang findet.

Andererseits verlangt Art. 32 DSGVO das Erreichen eines angemessenen Schutzniveaus und i.V.m. Art. 24 DSGVO die Erbringung des zugehörigen Nachweises. Das Schutzniveau wird aber gerade durch das Treffen von Schutzmaßnahmen erreicht, die folglich einen direkten Einfluss auf das formal festgestellte Schutzniveau haben müssen. Demnach muss es auch eine Bewertung des Risikos geben, welches nach der Umsetzung technischer und organisatorischer Maßnahmen verbleibt.

Deshalb wird angenommen, dass eine DSGVO-konforme Risikobewertung sich mit zwei Arten von Risiken befassen muss:

a. einem **intrinsischen Risiko**, welches neben der Schwere der Gefahr eine mit der Verarbeitungstätigkeit verknüpfte generische Eintrittswahrscheinlichkeit berücksichtigt;

b. einem **Restrisiko**, welches neben der Schwere der Gefahr eine Wahrscheinlichkeit berücksichtigt, die ausgehend von der generischen berücksichtigt, dass das Umsetzen von technischen und organisatorischen Maßnahmen die Realisierung der möglichen Gefahren beziehungswiese der potenziellen Schäden unwahrscheinlicher macht.

3.2. Potenzieller Schaden

Aus einer konkreten Verarbeitungstätigkeit können den betroffenen Personen, deren Daten verarbeitet werden, Schäden für ihre Rechtsgüter entstehen. Es gilt diese möglichen Schäden zu identifizieren und zu beschreiben. Hinweise hierzu finden sich in ErwG. 75 i.V.m. Art. 32 Abs. 2 DSGVO sowie in einschlägigen Veröffentlichungen, wie zum Beispiel {Datenschutzkonferenz [Hrsg.], Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, 2018}.

3.3.Gefahr

Während der potenzielle Schaden sich auf eine betroffene Person bezieht, muss bei der Betrachtung der Gefahr gem. § 64 BDSG insbesondere der Umfang der Datenverarbeitung beachtet werden, da der Gesamtschaden umso höher ist, je mehr Daten beziehungswiese Datensätze innerhalb der Verarbeitungstätigkeit verarbeitet werden. Die einer Verarbeitungstätigkeit immanente Gefahr besteht folglich aus einer geeigneten Kumulierung der einzelnen potenziellen Schäden.

3.4. Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit ist ein Maß für die Möglichkeit, dass eine identifizierte Gefahr tatsächlich eintritt.

Oben wurde bereits ausgeführt, dass zur Bewertung des intrinsischen Risikos eine mit der jeweiligen Verarbeitungstätigkeit zusammenhängende generische Eintrittswahrscheinlichkeit herangezogen werden muss, die zum Beispiel berücksichtigt, wer aus welchen Gründen mit welchem Aufwand den Schutz der verarbeiten Daten zu brechen versuchen könnte oder wie zuverlässig die bei der Verarbeitung eingesetzten Mittel und Prozesse grundsätzlich sind.

Daneben steht die Bewertung des Restrisikos, das eine Eintrittswahrscheinlichkeit berücksichtigt, welche technische und organisatorische Maßnahmen einbezieht, die zum Schutz der Verarbeitung etabliert wurden.

3.5. Risikobehandlung

Art. 32 Abs. 1 i.V.m. ErwG 78 DSGVO fordert die Gewährleistung eines dem Risiko angemessenen Schutzniveaus durch Maßnahmen. Hierdurch wird implizit eine Reduzierung des effektiven Restrisikos durch Maßnahmen vorgeschrieben. Andere sonst übliche Optionen der Risikobehandlung, wie zum Beispiel der Transfer oder die ausnahmsweise Akzeptanz auch kritischer Risiken, sieht der Datenschutz nicht vor.

3.6. Metriken

ErwG 76 gibt i.V.m. Art. 35 DSGVO den Hinweis, dass die Bewertung von Risiken durch die drei Kategorien „niedrig", „normal" und „hoch" erfolgen soll. Dem folgt auch das Kurzpapier zum Thema Risiko der Datenschutzkonferenz {Datenschutzkonferenz [Hrsg.], Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, 2018} sowie das Standard-Datenschutzmodell der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder {AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder [Hrsg.]: Das Standard-Datenschutzmodell. Version 2.0b vom 17.04.2020.} Bezüglich der Metriken zur Bewertung von potenziellen Schäden, Gefahren und Eintrittswahrscheinlichkeiten geben die DSGVO und das BDSG keine Hinweise. Allerdings macht die vorstehend erstgenannte Veröffentlichung hierzu passende Vorschläge. ▸

4. Modell zur Umsetzung

Kern des Modells zur risikobasierten Planung technischer und organisatorischer Maßnahmen nach Art. 32 DSGVO ist ein System zur Dokumentation der Maßnahmen in Verbindung mit den Ergebnissen der durchzuführenden Risikobewertung.

Die Durchführung der Risikobewertung und ebenso die regelmäßige Prüfung und Aktualisierung der Dokumentation sollten durch entsprechende Prozesse sichergestellt werden.

Abb. 3 zeigt die drei wesentlichen Bestandteile der Dokumentation, die nachfolgend erläutert werden.

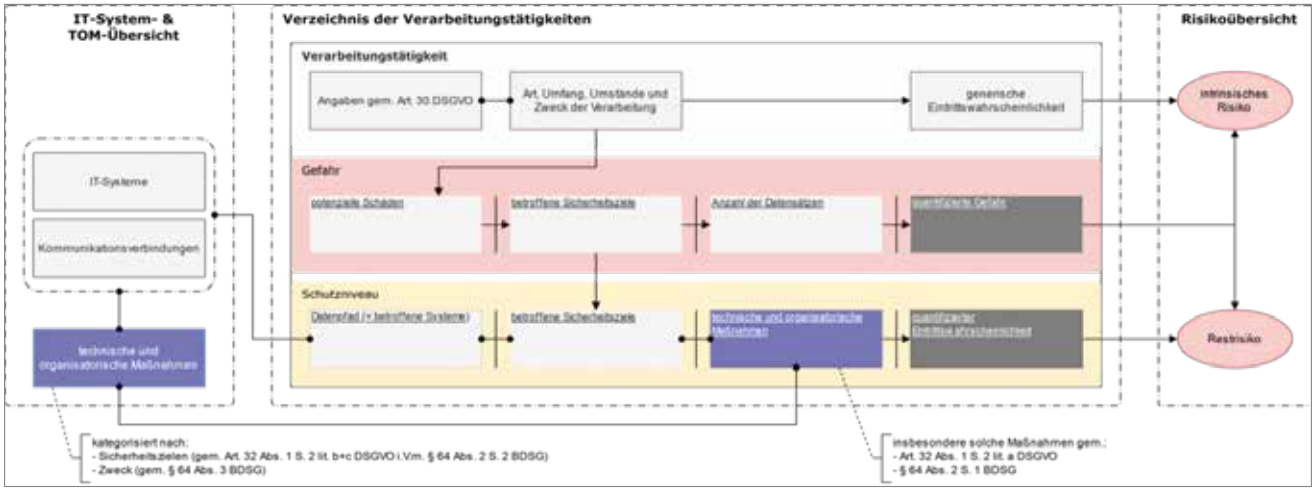


Abb. 3: Dokumentation der Risikobewertung und der technischen und organisatorischen Maßnahmen

4.1. IT-System- und TOM-Übersicht

Eine Verarbeitung personenbezogener Daten besteht aus einer Abfolge verschiedener Aktionen, die im Falle der automatisierten Verarbeitung von IT-Systemen durchgeführt werden. Dabei können verschiedene Systeme involviert sein, welche Daten über Kommunikationsverbindungen miteinander austauschen. Technische Maßnahmen zum Schutz der Verarbeitung haben in der Regel einen direkten oder indirekten Bezug zu einem oder mehreren der Systeme oder der Kommunikationsverbindungen.

Auch wenn für jede Verarbeitungstätigkeit explizit dokumentiert werden sollte, welche Systeme und Verbindungen für die Durchführung genau dieser Tätigkeit genutzt werden, bietet es sich aus Gründen der Übersichtlichkeit und Vereinfachung an, eine zentrale Übersicht der IT-Systeme und Kommunikationsverbindungen zu führen. An anderer Stelle beziehungsweise in anderen Dokumenten kann dann mit Referenzen auf diese zentrale Übersicht gearbeitet werden.

Die zentrale Dokumentation der Systeme und Verbindungen ist darüber hinaus ein geeigneter Ort, um die technischen und organisatorischen Maßnahmen in einer Form zu dokumentieren, aus der klar hervorgeht, auf welche Systeme oder Verbindung sich eine Maßnahme bezieht und welchem Sicherheitsziel sie dient.

4.2. Verzeichnis der Verarbeitungstätigkeiten

Die Erweiterung des Verzeichnisses der Verarbeitungstätigkeiten spielt eine zentrale Rolle, da das Verzeichnis genau die Instanz ist, die Art, Umfang, Umstände und Zweck der Verarbeitung beschreibt. Für jede Verarbeitungstätigkeit wird dokumentiert, welche Schäden den betroffenen Personen aufgrund der konkreten Verarbeitung ihrer Daten entstehen können und durch den Bruch welches Sicherheitsziels sich dies realisieren könnte. Unter Berücksichtigung des Umfangs der verarbeiteten Daten lassen sich die identifizierten Schäden zu einer oder mehreren Gefahren zusammenfassen, die mit dieser Tätigkeit für Rechtsgüter der betroffenen Personen verbunden sind.

Mittels einer geeigneten Risikometrik lässt sich die quantifizierte Gefahr und eine für die gesamte Verarbeitungstätigkeit bestimmte generische Eintrittswahrscheinlichkeit zu einem Maß für das dieser Verarbeitungstätigkeit immanenten Risikos kombinieren.

Mit Hilfe der IT-Systemübersicht kann weiterhin der Datenpfad beschrieben werden, der in der Regel eine Liste der IT-Systeme und Verbindungen ist, die im Rahmen der Verarbeitungstätigkeit eingesetzt werden.

Nun wird für den konkreten Datenpfad bestimmt, wie wahrscheinlich ein Bruch eines der jeweils zu berücksichtigenden Sicherheitsziele ist, wobei genau die technischen und organisatorischen Maßnahmen berücksichtigt werden, die auf diesem Datenpfad für die Gewährleistung der jeweiligen Sicherheitsziele sorgen. Auf diese Weise folgt die Bewertung der Eintrittswahrscheinlichkeit der Systematik, die im klassischen IT-Sicherheitsmanagement eingesetzt wird und kann auch als Maß der Widerstandsfähigkeit eines oder mehrerer Systeme oder Verbindungen bezüglich eines Sicherheitsziels gesehen werden.

Schließlich ergibt die Kombination der quantifizierten Gefahren und der so bewerteten Eintrittswahrscheinlichkeiten das verbleibende Restrisiko.

4.3. Risikoübersicht

Die für die einzelnen Verarbeitungstätigkeiten identifizierten und bewerteten intrinsischen und Restrisiken können schließlich in einer Risikoübersicht zentral dokumentiert werden. Gegebenenfalls kann das Erzeugen der Risikoübersicht aus den einzelnen Verarbeitungstätigkeiten automatisiert erfolgen.

Ein angemessenes Schutzniveau ist nun genau dann erreicht, wenn die getroffenen technischen und organisatorischen Maßnahmen ausreichen, die Eintrittswahrscheinlichkeiten, auf welche sie einen Einfluss haben, derart zu reduzieren, dass alle identifizierten und bewerteten Restrisiken unter einem festgelegten Wert liegen – bewertet man die Risiken zum Beispiel mittels der erwähnten Kategorien: „gering", „normal" und „hoch", so könnte festgelegt werden, dass geringe und normale Risiken akzeptabel sind, hohe Risiken aber zwingend reduziert werden müssen. Auch ist denkbar, dass für die Verarbeitung von besonderen Kategorien von personenbezogenen Daten gem. Art. 9 DSGVO ein niedrigerer Schwellenwert festgelegt wird.

4.4. Überprüfung der Wirksamkeit

Um die in Art. 32 Abs. 1 HS. 2 lit. d i.V.m. Art. 24 Abs. 1 S. 2 DSGVO geforderte regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der getroffenen technischen und organisatorischen Maßnahmen sicherzustellen, bleibt dem Verantwortlichen die Durchführung technischer Audits und entsprechender Sicherheitstests, welche prüfen, ob die jeweiligen Maßnahmen in dem in der Risikobewertung angegeben Maß in ihrer konkreten Umsetzung tatsächlich zur Gewährleistung der zu berücksichtigenden Sicherheitsziele beitragen.

Über den Autor

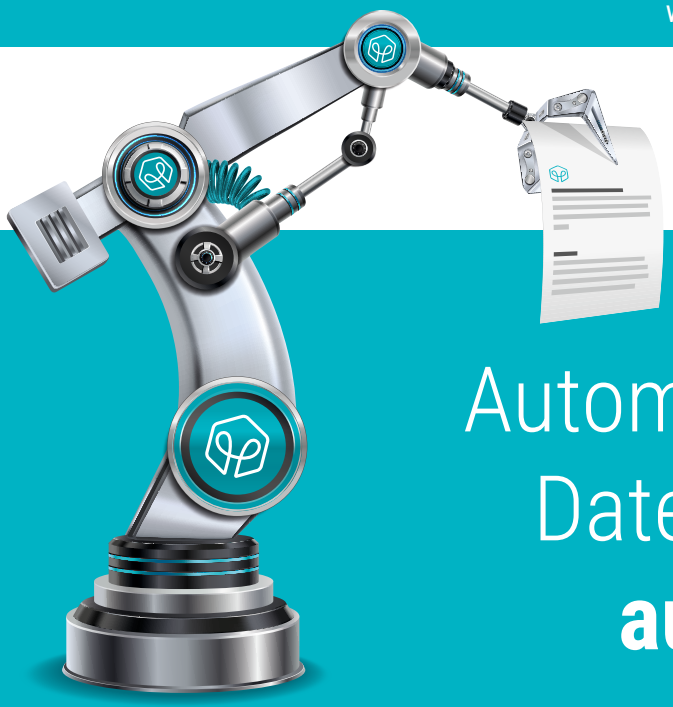
Dr. Gunther Schlöffel

ist Vorstand der pen.sec AG, bei der er die Geschäftsfelder Penetrationstests und Datenschutz betreut.

pen.sec
Protecting Your Assets

Anzeige

www.audado.eu



audado

Automatisierung.
Datenschutz.
audado.

Jetzt **10%** Rabatt auf unsere **Datenschutz-Module** für BvD-Mitglieder!

Rabattcode im Mitgliederbereich

Intelli Revolution GmbH | Überseeallee 1 | 20457 Hamburg | info@intelli-revolution.de

ZUVERLÄSSIGKEIT UND QUALIFIKATION DES DATENSCHUTZBEAUFTRAGTEN

Landesarbeitsgericht Mecklenburg-Vorpommern konkretisiert die Anforderungen

Dr. Carlo Piltz und Philipp Quiel

A. Gegenstand der Entscheidung und Relevanz

Mit Urteil vom 25.2.2020 (Az. 5 Sa 108/19) hat das Landesarbeitsgericht Mecklenburg-Vorpommern (im Folgenden „LAG") einige relevante Aussagen zu wichtigen Themenkomplexen getroffen, die für die Tätigkeit von Datenschutzbeauftragten von zentraler Bedeutung sind. Zum einen hinsichtlich der Anforderungen an die fachliche Qualifikation und bezüglich des Fachwissens. Zum anderen war Gegenstand der Entscheidung, welche Voraussetzungen für eine Abberufung eines Datenschutzbeauftragten gelten. In diesem Beitrag wird die Argumentation des LAG näher betrachtet. Obwohl für die Entscheidung des Gerichts noch das Landesdatenschutzrecht in alter Fassung maßgeblich war, bestehen viele Parallelen zu den nunmehr geltenden Vorgaben der DSGVO (und soweit anwendbar) des BDSG. Zur Veranschaulichung der Übertragbarkeit und der damit einhergehenden Praxisrelevanz des Urteils werden an ausgewählten Stellen Vergleiche zu den Vorgaben der DSGVO und des BDSG gemacht.

B. Sachverhalt

In dem Verfahren vor dem LAG stritten der intern benannte Datenschutzbeauftragte (Kläger) und die beklagte Körperschaft des öffentlichen Rechts (Beklagte) über die Wirksamkeit der zuvor erfolgten Abberufung des Datenschutzbeauftragten.

Die Beklagte betreibt ein Universitätsklinikum mit mehr als 4100 Beschäftigten. Zur Unternehmensgruppe gehören weitere elf Gesellschaften mit insgesamt rund 900 Beschäftigten. Der Datenschutzbeauftragte ist Volljurist und war seit 2007 bei der Beklagten zunächst als Personaldezernent tätig. Mit Wirkung zum 1.1.2015 schlossen die Parteien einen Änderungsvertrag, in dem

unter anderem die Bestellung des Klägers geregelt war. Auf Anfrage des Datenschutzbeauftragten beim Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern gab die Behörde an, dass der Arbeitsumfang an der Universitätsklinik als Vollzeitbeschäftigung einzustufen sei. Daraufhin schlossen die Parteien einen weiteren Änderungsvertrag, der vorsah, dass der Kläger im Umfang von 25 Prozent seiner Arbeitszeit als Justiziar sowie als 2. Abfallbeauftragter weiterbeschäftigt wird. Im Übrigen wurde eine Freistellung zu 75 Prozent der Arbeitszeit für Aufgaben des behördlichen Datenschutzbeauftragten sowie des Konzernbeauftragten für den Datenschutz festgelegt.

Als Datenschutzbeauftragter veranstaltete der Kläger interne Datenschutzkonferenzen, zu denen er die lokalen Datenschutz-Verantwortlichen einlud. Im Rahmen von innerbetrieblichen Fortbildungen bot er zudem Schulungen zu verschiedenen Themen des Datenschutzes an. Er wirkte auch in verschiedenen Gremien und Arbeitskreisen mit. Seit 2017 war der Kläger zudem Mitglied des Gesamtpersonalrats der Beklagten.

Im Januar 2018 führte die Beklagte mit dem Kläger ein Gespräch zum Stand der Umsetzung der DSGVO im eigenen Haus und bei den Tochtergesellschaften. Der Kläger nahm hierzu mit Schreiben vom 31.1.2018 Stellung und berichtete über die noch laufenden Gesetzgebungsverfahren im Land Mecklenburg-Vorpommern zur Anpassung des allgemeinen und des bereichsspezifischen Datenschutzrechts, insbesondere des Datenschutz- und des Landeskrankenhausgesetzes. Des Weiteren verwies er auf einen von ihm verfassten Aufsatz zur DSGVO in der Zeitschrift „*f&w, führen und wirtschaften im Krankenhaus*", Ausgabe 2/17. Im vorletzten Satz des Schreibens heißt es: „*Die konkrete Umsetzung der Datenschutzgesetze des Landes kann durch die Datenschutz-Verantwortlichen denklogisch erst nach Inkrafttreten der Gesetze erfolgen.*"

Da die Beklagte und andere Unternehmen im Konzern nicht mit der Herangehensweise des Datenschutzbeauftragten einverstanden waren, widerriefen die Tochtergesellschaften der Beklagten mit Schreiben vom 19.2.2018 mit sofortiger Wirkung die Bestellung des Klägers zum Konzern- und zum behördlichen Datenschutzbeauftragten. Mit Schreiben vom 20.2.2018 widerrief auch die Beklagte mit sofortiger Wirkung die Bestellung zum Konzerndatenschutzbeauftragten.

Am 27.2.2018 führte die Beklagte mit dem Kläger erneut ein Gespräch, in dem sie ihm jegliche Tätigkeit als Datenschutzbeauftragter für ihre Gesellschaft und die Tochtergesellschaften untersagte. Die Beklagte widerrief mit weiteren Schreiben vorsorglich erneut die Bestellung zum Konzern- und zum behördlichen Datenschutzbeauftragten. Ebenso erklärten zehn Tochtergesellschaften nochmals den Widerruf der Bestellung. Danach führte die Beklagte mit dem Kläger ein Personalgespräch zu Vorwürfen, er habe in kollusivem Zusammenwirken rechtswidrig eine erhöhte Altersversorgung für einen ehemaligen kaufmännischen Vorstand eingerichtet und bei der eigenen Versorgungszusage ebenfalls rechtswidrig die Summe zu seinen Gunsten erhöht. Anschließend stellte die Beklagte den Datenschutzbeauftragten unwiderruflich von der Arbeit frei und erteilte ihm Hausverbot.

Die Beklagte begründet ihre Widerrufe damit, dass der Kläger es vollständig unterlassen habe, auf eine Umsetzung der Vorgaben aus der DSGVO hinzuwirken. Die Umsetzung der DSGVO und der ergänzenden Bestimmungen sei mit einem erheblichen zeitlichen und organisatorischen Aufwand verbunden. Zunächst sei eine Bestandaufnahme der eigenen Datenverarbeitung vorzunehmen. Sodann seien der Anpassungsbedarf festzustellen und konkrete Maßnahmen daraus abzuleiten sowie umzusetzen. Komme die Beklagte dem nicht nach, müsse sie mit erheblichen Sanktionen rechnen. Der Datenschutzbeauftragte habe die Umsetzung der DSGVO proaktiv zu begleiten und eigene Vorschläge einzubringen. Mit dem Schreiben vom 31.1.2018 habe der Kläger zu erkennen geben, dass er nicht gewillt sei, seinen Verpflichtungen nachzukommen. Darüber hinaus fehle dem Kläger die erforderliche Zuverlässigkeit, da er bei seiner eigenen Altersversorgung eine Erhöhung der Beiträge von 3,9 % des anrechenbaren Nettoaufkommens auf 9,65 % veranlasst habe. Der monatliche Beitrag habe sich dadurch von 275,68 Euro auf 671,54 Euro erhöht. Damit habe er sich einer strafbewehrten Untreue schuldig gemacht.

In der Vorinstanz hatte das Arbeitsgericht Stralsund der Klage des Datenschutzbeauftragten stattgegeben. Die Widerrufe der Bestellung zum Datenschutzbeauftragten sowie Konzerndatenschutzbeauftragten seien unwirksam. Angesichts der unabhängigen Stellung des Datenschutzbeauftragten sei eine Abberufung nur aus schwerwiegenden Gründen zulässig.

C. Entscheidung des LAG

Das LAG entschied genauso wie die Vorinstanz, dass die Bestellung des Klägers zum behördlichen Datenschutzbeauftragten und zum Konzerndatenschutzbeauftragten nicht wirksam widerrufen wurden. Das LAG bezieht sich bei seiner Entscheidung auf den damaligen § 20 Abs. 2 DSG M-V a.F. Es sei für die Rechtmäßigkeit eines ▸

Widerrufs (ebenso wie bei einer Kündigung) das zum Zeitpunkt des Zugangs der Widerrufserklärung geltende Recht anzuwenden. Gemäß § 20 Abs. 2 DSG M-V konnte die Bestellung zum behördlichen Datenschutzbeauftragten schriftlich widerrufen werden, wenn ein Interessenkonflikt mit seinen anderen dienstlichen Aufgaben eintritt oder sonst ein wichtiger Grund in entsprechender Anwendung von § 626 BGB vorliegt. Die Regelung ähnelt also stark der aktuell geltenden Vorgabe in § 6 Abs. 4 BDSG, die über den Verweis in § 38 Abs. 2 BDSG auch für Unternehmen anwendbar sind.

1. Interessenkonflikt und wichtiger Grund

Mit Verweis auf die Rechtsprechung des Bundesarbeitsgerichts (BAG, Urteil vom 5.12.2019 – 2 AZR 223/19, Rn. 25; BAG, Urteil vom 23.3.2011 – 10 AZR 562/09, Rn. 24) stellt das LAG zunächst fest, dass ein Interessenkonflikt besteht, wenn der Datenschutzbeauftragte in erster Linie seine eigene Tätigkeit kontrollieren muss. Die Mitgliedschaft im Betriebsrat ist aber grundsätzlich mit der Tätigkeit eines Datenschutzbeauftragten vereinbar (BAG, Urteil vom 23.3.2011 – 10 AZR 562/09, Rn. 25).

Ein wichtiger Grund (in entsprechender Anwendung von § 626 BGB) ist nach Ansicht des LAG dann gegeben, wenn Tatsachen vorliegen, aufgrund derer dem Arbeitgeber unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile ein weiterer Einsatz des Mitarbeiters in der Funktion des Datenschutzbeauftragten nicht mehr zugemutet werden kann. Als wichtige Gründe kommen insbesondere solche in Betracht, die mit der Funktion und der Tätigkeit des Datenschutzbeauftragten zusammenhängen und eine weitere Ausübung dieser Tätigkeit unmöglich machen oder sie zumindest erheblich gefährden. Beispielsweise ein Geheimnisverrat oder eine dauerhafte Verletzung der datenschutzrechtlichen Kontrollpflichten. Ein wichtiger Grund läge jedenfalls nicht bereits deshalb vor, weil ein Unternehmen einen externen Dienstleister oder eine andere Person für besser geeignet hält als ihren aktuellen Datenschutzbeauftragten.

An dieser Stelle ist anzumerken, dass gemäß Art. 38 Abs. 3 S. 2 DSGVO ein Datenschutzbeauftragter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden darf. Im BDSG gibt es zudem mit §§ 6 Abs. 4 und 38 Abs. 2 BDSG Vorschriften, die den vom LAG angewendeten landesrechtlichen Regelungen entsprechen. Die Aussagen des LAG können also auch zur Auslegung der aktuellen Rechtslage herangezogen werden.

2. Erforderliche Sachkunde und Zuverlässigkeit

Hinsichtlich der Anforderungen an die Sachkunde und Zuverlässigkeit verweist das LAG auf § 20 Abs. 1 S. 3 DSG M-V a.F. Danach durfte zum Datenschutzbeauftragten nur bestellt werden, wer die zur Erfüllung seiner Aufgabe erforderliche Sachkunde und Zuverlässigkeit besitzt. Sind diese Voraussetzungen im Verlauf weggefallen, so das LAG, ist es dem Arbeitgeber grundsätzlich nicht zumutbar, den Betreffenden weiterhin in der Funktion des Datenschutzbeauftragten zu belassen, zumal dieser sich dadurch selbst gesetzeswidrig verhalten würde.

Nach Ansicht des LAG besaß der Kläger hier sowohl die erforderliche Sachkunde als auch die erforderliche Zuverlässigkeit zur Erfüllung der dem behördlichen Datenschutzbeauftragten obliegenden Aufgaben.

Art. 37 Abs. 5 DSGVO sieht vor, dass der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikationen und insbesondere des Fachwissens benannt wird, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben. § 5 Abs. 3 BDSG hat denselben Regelungsinhalt.

a. Sachkunde

Das LAG musste zunächst die Frage beantworten, welche Anforderungen das Landesdatenschutzrecht an die Sachkunde und Fachkenntnis des Datenschutzbeauftragten stellt.

Das Gericht verweist darauf, dass das Gesetz die Tätigkeit des Datenschutzbeauftragten nicht an eine bestimmte Ausbildung oder näher bezeichnete Fachkenntnisse knüpft. Welche Sachkunde hierfür erforderlich ist, richte sich insbesondere nach der Größe der zu betreuenden Organisationseinheit, dem Umfang der anfallenden Datenverarbeitungsvorgänge, den eingesetzten IT-Verfahren, dem Typus der anfallenden Daten. Regelmäßig seien Kenntnisse des Datenschutzrechts, zur Technik der Datenverarbeitung und zu den betrieblichen Abläufen erforderlich. Das LAG geht daher deutlich erkennbar von einem auf den Einzelfall anzupassenden und damit formbaren Sachkundebegriff aus.

Zudem vertritt das LAG die Ansicht, dass der Datenschutzbeauftragte nur in einem Teilbereich über eine eigene Qualifikation verfügen müsse und es genügt, wenn er im Übrigen auf fachkundige Mitarbeiter zurückgreifen kann. Das bedeutet, dass der Datenschutzbeauftragte für spezielles Wissen im juristischen oder auch technischen Bereich durchaus auf interne oder externe Beratung zurückgreifen kann, dies jedoch nichts an seiner eigenen Sachkunde ändert. Hierauf verweist das LAG auch ausdrücklich im konkreten Fall. Zu den technischen Fragen der Datenverarbeitung konnte sich der Kläger nämlich bei dem stellvertretenden Datenschutzbeauftragten informieren, der ein Informatiker ist.

Das LAG vertritt die Auffassung, dass Fortbildungen zu den neuen technischen Entwicklungen und Gesetzesänderungen und Entwicklungen in der Rechtsprechung unerlässlich seien. Die DSGVO schreibt in Art. 38 Abs. 2 nunmehr vor, dass dem Datenschutzbeauftragten die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung gestellt werden. Das Vorgängergremium des Europäische Datenschutzausschusses interpretiert dies ähnlich wie das LAG. In den Leitlinien in Bezug auf Datenschutzbeauftragte (WP 243 rev.01) sehen die europäischen Datenschutzbehörden es ebenfalls für erforderlich an, dass Datenschutzbeauftragte ihr Fachwissen kontinuierlich erweitern: „*Dem Datenschutzbeauftragten sollte Gelegenheit gegeben werden, sich in Bezug auf Entwicklungen im Bereich des Datenschutzes auf dem aktuellen Stand zu halten. Ziel sollte dabei sein, die Fachkompetenz der Datenschutzbeauftragte kontinuierlich zu erhöhen, und Datenschutzbeauftragte sollten ermuntert werden, an Fortbildungsveranstaltungen über Datenschutz und an sonstigen Formen der beruflichen Weiterbildung (Datenschutzforen, Workshops usw.) teilzunehmen*." Der Kläger war als Volljurist nach Ansicht des LAG ohne Weiteres in der Lage sich mit dem einschlägigen Datenschutzrecht vertraut zu machen und dieses praktisch anzuwenden. Aufgrund der vorangegangenen langjährigen Tätigkeit als Personaldezernent waren ihm die wesentlichen Grundzüge des Datenschutzes bereits geläufig. Das LAG verwies zudem auf die Veröffentlichung des Klägers, die ebenfalls für sein Fachwissen sprachen.

Wie oben bereits erwähnt, enthalten die DSGVO und das BDSG keine detaillierten Vorgaben dazu, wodurch bei einem Datenschutzbeauftragten eine hinreichende Sachkunde vorliegt. In einigen Entwürfen des Verordnungstextes waren die Vorgaben zum Teil explizierter ausgestaltet. Letztendlich hat sich der Verordnungsgeber aber dafür entschieden, den Mitgliedstaaten Gestaltungsspielraum bei der Spezifizierung der Anforderungen an die Sachkunde zu überlassen. Im Kern geht es wohl stets darum, dass beim Datenschutzbeauftragten das für die Erfüllung seiner konkreten, in einem Unternehmen zu bewältigenden Aufgaben genügend Wissen – unter Einbeziehung von möglichen Unterstützungen durch Sachkunde anderer Personen – vorhanden ist oder eingeholt und verwertet werden kann.

Bei der Sachkunde kann es auch Abweichungen in verschiedenen Branchen geben: Wenn das Unternehmen, für das der Datenschutzbeauftragte bestellt ist, in einer Branche tätig ist, auf die spezielle rechtliche Vorgaben anwendbar sind (so etwa bei Krankenhäusern, Sozialeinrichtungen aber auch Banken), die Einfluss auf Datenverarbeitungen der Unternehmen haben, benötigt ein Datenschutzbeauftragter dieses Unternehmens eine andere Sachkunde als bei einer Supermarktkette. Ebenso haben auch die Größe und Struktur des Unternehmens einen Einfluss auf die Sachkunde. In einem größeren Unternehmen wird man beispielsweise auch Management- und Kommunikationsfähigkeiten dazuzählen können.

b. Zuverlässigkeit

Auch die erforderliche Zuverlässigkeit sah das LAG als gegeben an. Nach Ansicht des LAG muss der Datenschutzbeauftragte auch die Gewähr bieten, dass er seinen Aufgaben gewissenhaft nachkommt und nicht gegen seine Pflichten als Datenschutzbeauftragter (z.B. gegen seine Verschwiegenheitspflicht) verstößt. Eine schwerwiegende Verletzung allgemeiner arbeitsvertraglicher Pflichten kann die Zuverlässigkeit infrage stellen. Hierzu zählen laut dem LAG beispielsweise Diebstahl, Unterschlagung, vorsätzliche Rufschädigung, Tätlichkeiten gegen andere Beschäftigte.

Die Zuverlässigkeit ist nach Ansicht des LAG unter Berücksichtigung von Sinn und Zweck der Bestellung eines Datenschutzbeauftragten zu bewerten. Der Datenschutzbeauftragte hat die Aufgabe, eine wirkungsvolle Eigenkontrolle der datenschutzrechtlichen Vorschriften sicherzustellen, um dadurch zugleich öffentliche Kontrollstellen zu entlasten. Die zum Datenschutzbeauftragten bestellte Person muss eine wirksame Selbstkontrolle gewährleisten können. Bei einem internen Datenschutzbeauftragten lässt sich dessen Stellung nicht vollständig von dem zugrundeliegenden Arbeitsverhältnis trennen. Eine schwerwiegende Verletzung arbeitsvertraglicher Pflichten kann daher dazu führen, dass eine zuverlässige Ausübung der datenschutzrechtlichen Selbstkontrolle nicht mehr möglich ist.

Besonders relevant an dieser Begründung des LAG ist die Verknüpfung zwischen Arbeitsverhältnis und der Rolle als Datenschutzbeauftragter. Eine Pflichtverletzung im Arbeitsverhältnis kann sich auf die Tätigkeit als Datenschutzbeauftragter und die erforderliche Zuverlässigkeit auswirken. Es scheint daher eine Betrachtung zweier Pflichtenebenen geboten: zum einen die (gesetzlichen) Pflichten als Datenschutzbeauftragter, zum anderen die arbeitsvertraglichen Pflichten. Die DSGVO macht keine Vorgaben dazu, wie und unter welchen Voraussetzungen ein Datenschutzbeauftragter abberufen werden darf. Es gibt in Art. 38 Abs. 3 S. 2 DSGVO lediglich allgemeine Vorgaben dafür, aus welchen Gründen ein Datenschutzbeauftragter nicht abberufen werden darf. In § 6 Abs. 4 BDSG hat der deutsche Gesetzgeber an die in der alten, vor der DSGVO anwendbaren Fassung angeknüpft. Es ist nach dieser Vorschrift in entsprechender Anwendung des § 626 BGB dann zulässig einen Datenschutz- ▸

beauftragten abzuberufen, wenn Tatsachen vorliegen, welche zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen.

Nach Ansicht des LAG hat der Kläger hier aber weder seine Pflichten als Datenschutzbeauftragter noch seine Pflichten aus dem Arbeitsverhältnis schwerwiegend verletzt. Zum einen habe der Kläger seine Aufgaben als Datenschutzbeauftragter nicht vernachlässigt. Das LAG verweist hier ausdrücklich darauf, dass – angesichts der Größe des zu betreuenden Bereichs – es zwingend erforderlich sei, bei der Tätigkeit als Datenschutzbeauftragter Schwerpunkte zu setzen. Der Kläger habe vorliegend auf die Einhaltung von Datenschutzvorschriften hingewirkt. Er habe zudem die Beschäftigten mit den Vorschriften des Datenschutzes vertraut gemacht. Für eine Schwerpunktsetzung bei der Ausübung der Tätigkeiten des Datenschutzbeauftragten gibt es auch innerhalb der DSGVO einen Anhaltspunkt. In Art. 39 Abs. 2 DSGVO heißt es wie folgt: „*Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.*“ Diese Vorschrift ist so zu verstehen, dass der Datenschutzbeauftragte seine Aufgaben entsprechend des von der jeweiligen Datenverarbeitung ausgehenden Risikos priorisieren kann.

Das oben erwähnte Schreiben vom 31.1.2018 sieht das LAG nicht als Grund an, um an der Zuverlässigkeit zu zweifeln. Der Kläger habe darin nicht erklärt, seinen Verpflichtungen nicht nachkommen zu wollen. Die Einhaltung des Datenschutzrechts unter Berücksichtigung der einschlägigen Rechtsprechung ist nämlich zunächst Aufgabe der Beklagten als Betreiberin der Kliniken. Der Kläger als Datenschutzbeauftragter sei ein Kontrollorgan. Er hat zwar bei der Umsetzung der erforderlichen Maßnahmen zu unterstützen. Die Umsetzung selbst bleibt jedoch Aufgabe der Beklagten. Das Schreiben aus Januar 2018 enthalte ausschließlich Informationen zum Stand der Gesetzgebung. Auf die zu erwartenden rechtlichen Änderungen hatte sich der Kläger bereits vorbereitet, indem er sich mit der DSGVO auseinandergesetzt und das Gesetzgebungsverfahren zum Landesrecht verfolgt hatte. Dies ist ein wichtiger Hinweis des LAG: Datenschutzbeauftragte müssen die aktuellen Entwicklungen, gerade auch auf rechtlicher Ebene in der Rechtsprechung und Gesetzgebung verfolgen.

Laut dem LAG habe der Kläger keine allgemeinen Pflichten aus dem Arbeitsverhältnis verletzt, die einem weiteren Einsatz in der Funktion des Datenschutzbeauftragten entgegenstehen. Der Kläger habe die Beklagte nicht zielgerichtet zum eigenen Vorteil geschädigt oder dieses versucht. Er habe sich nicht bewusst über vertragliche, tarifvertragliche oder gesetzliche Vorschriften hinweggesetzt, um sich selbst rechtswidrig zu begünstigen. Das Vertrauen in ein rechtskonformes Handeln des Klägers sei daher nicht zerstört.

D. Fazit

Die Entscheidung des LAG ist sehr praxisrelevant. Häufig entstehen bei der Abberufung von Datenschutzbeauftragten Rechtsstreite um die Zulässigkeit. Obwohl das Gericht eigentlich nicht direkt zur DSGVO geurteilt hat und eher landesrechtliche Vorgaben maßgeblich waren, enthält das Urteil viele Argumente, die man auf die aktuelle Rechtslage unter der DSGVO und dem BDSG übertragen kann. Deswegen ist das hier besprochene Urteil hilfreich für die Auslegung der aktuell geltenden Vorgaben.

Über die Autoren

Dr. Carlo Piltz
ist Rechtsanwalt bei reuschlaw Legal Consultants, Berlin

Philipp Quiel
ist Wirtschaftsjurist bei reuschlaw Legal Consultants, Berlin

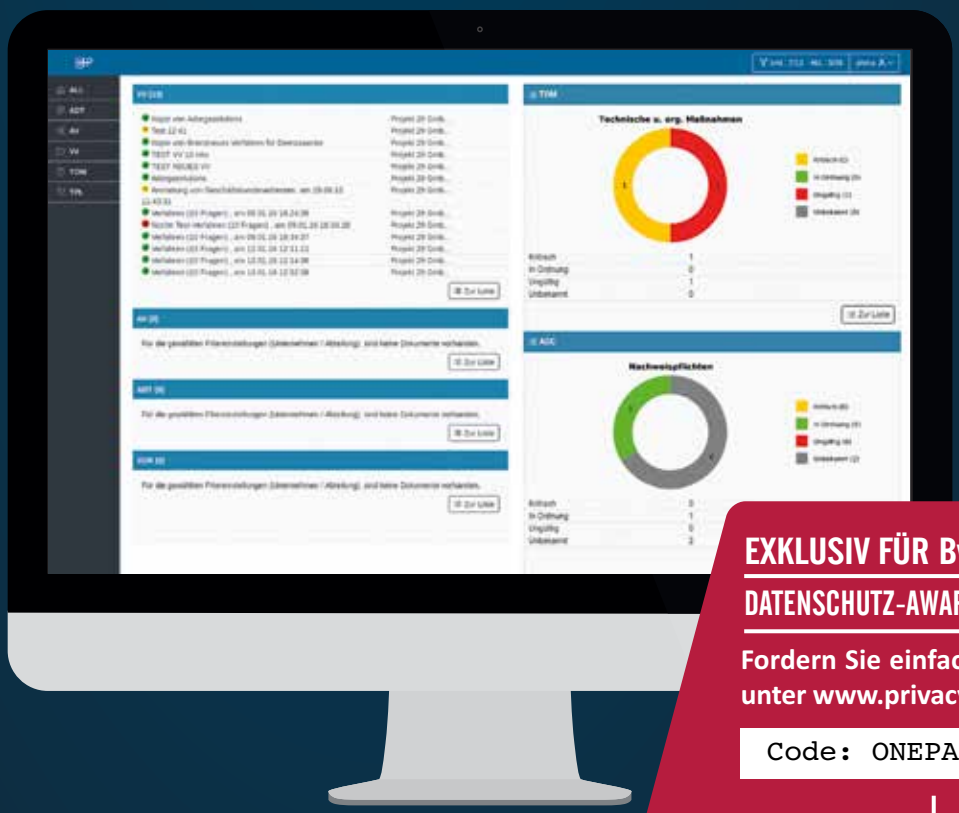
▶ www.reuschlaw.de

reuschlaw Legal Consultants

Anzeige

PRIVACYSOFT

IHR DSB-MULTI-TOOL FÜR ALLE AUFGABEN IM DATENSCHUTZMANAGEMENT



EXKLUSIV FÜR BvD-MITGLIEDER

DATENSCHUTZ-AWARENESS-ONEPAGER

Fordern Sie einfach und kostenlos unter www.privacysoft.de an.

Code: ONEPAGERBVD2020

BvD e.V. MITGLIED DATENSCHUTZ GESTALTEN

KOMPLETTE DATENSCHUTZDOKUMENTATION

EXTRA VORLAGEN UND CHECKLISTEN

NEUES AUDITMODUL

BEWÄHRTE ONLINE-SCHULUNGEN

MEHRSPRACHIG // DE / EN / FR

ZUSAMMENARBEIT // TICKET

Ab sofort haben Sie die Möglichkeit eine ganz persönliche kostenlose Präsentation dieser praxisbewährten Datenschutzmanagement Software zu bekommen. Wir verschaffen Ihnen bei einem kleinen Rundgang durch unsere Lösung spannende Einblicke und interessante Perspektiven.

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

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

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

DATENSCHUTZ KNOW-HOW SEIT 1996

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

KEINE AUFTRAGSVERARBEITUNG DURCH STEUERBERATER

Steuerberatungsgesetz enthält entsprechende Klarstellung

Rudi Kramer und Nicole Schmidt

Die Bestimmungen der Datenschutz-Grundverordnung (DSGVO) gelten seit dem 25. Mai 2018 europaweit. In der datenschutzrechtlichen Bewertung von Sachverhalten hat sich seither einiges verändert. Unbestimmte, auslegungsbedürftige Rechtsbegriffe haben sich konkretisiert, die Aufsichtsbehörden haben klarstellende Kurzpapiere und Orientierungshilfen veröffentlicht und der Gesetzgeber hat an der einen oder anderen Stelle korrigierend eingegriffen.

Das Thema war unter dem alten Recht bereits geklärt, mit dem Inkrafttreten der DSGVO kam die Diskussion zur datenschutzrechtlichen Bewertung der Lohn und Gehaltsbuchführung durch den Steuerberater neu auf. Im Zentrum der Auseinandersetzung stand die Frage, ob die vorgenannten Tätigkeiten als Auftragsverarbeitung im Sinne des Art. 28 DSGVO zu bewerten sind. Wesentliches Merkmal der Auftragsverarbeitung ist die Verarbeitung personenbezogener Daten nur auf dokumentierte Weisung des Verantwortlichen. Gleichzeitig sind Steuerberater wegen der berufsrechtlichen Vorgaben des § 57 Abs. 1 Steuerberatungsgesetz (StBerG) grundsätzlich in Ausübung ihres Mandats weisungsfrei.

Meinungsbildung der Aufsichtsbehörden

Anfang 2018 positionierte sich die Datenschutzkonferenz (DSK) in dem Kurzpapier Nr. 13[1] zur Auftragsverarbeitung.

Anhang A enthält zunächst die Bewertung, dass DV-technische Arbeiten für die Lohn und Gehaltsabrechnung oder die Finanzbuchhaltung durch Rechenzentren regelmäßig als Auftragsverarbeitung zu bewerten sind. Im Gegensatz dazu handelt es sich gemäß den Ausführungen in Anhang B nicht um eine Auftragsverarbeitung, sondern um die Inanspruchnahme externer Fachleistungen bei einem eigenständigen Verantwortlichen, wenn ein Berufsgeheimnisträger (Steuerberater, Rechtsanwalt, Wirtschaftsprüfer) mit der Verarbeitung von personenbezogenen Daten betraut wird. Die Bewertung der Non-Auftragsverarbeitung der Steuerberater in den Fällen der Lohn- und Gehalts- sowie der Finanzbuchhaltung griff die Bundessteuerberaterkammer (BStBK)[2] auf und führte als ergänzendes Argument das Berufsrecht an. Ausgehend von der vollen Verantwortung, die der Steuerberater in Ausübung seines Mandates trägt, ist dies nicht mit einer weisungsabhängigen Tätigkeit nach den Vorgaben des Mandanten in Einklang zu bringen. Ausfluss der Weisungsfreiheit ist in der Konsequenz auch die vollumfängliche Haftung bei der Falschberatung. Auch rein faktisch gesehen erweist sich die Pflicht zur Erteilung von Weisungen des Auftraggebers gegenüber dem Steuerberater als nicht erfüllbare Forderung. Es erfolgt ja gerade eine Auslagerung der Lohn- und Gehaltsbuchführung an den Steuerberater mangels einschlägiger Fachkenntnisse durch den Auftraggeber. Es wäre insofern widersinnig, wenn der Auftraggeber dem Steuerberater

[1] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf, Abruf: 06.07.2020, S. 4.

[2] Kalina-Kerschbaum, DStR-Kompakt, DStR Nr. 47/2018, S. XIV.

konkrete Hinweise zur Umsetzung der jeweiligen Buchführung erteilen würde.

Verschiedene Landesdatenschutzbeauftragte haben sich seit 2018 ebenfalls mit Beiträgen an der Diskussion beteiligt. Die Veröffentlichungen reichen von klarer Zustimmung zur Auftragsverarbeitung über vermittelnde Positionen bis hin zu vollkommener Ablehnung des Vorliegens der Voraussetzungen bei einer Übernahme der Lohnbuchführung durch den Steuerberater. So führte Landesbeauftragte für den Datenschutz und Informationsfreiheit Baden-Württemberg in seinem 34. Tätigkeitsbericht[3] aus, dass nur eine Auftragsverarbeitung die Tätigkeiten des Steuerberaters in datenschutzrechtlicher Weise richtig abbilden könne. Aus einem Beschluss des Bundesverfassungsgerichts vom 27. Januar 1982 leitete er ab, dass es sich bei der laufenden Lohnbuchhaltung um rein mechanische Verarbeitungsvorgänge handele, die keiner besonderen Qualifikation bedürfen. Infolgedessen bestimme der Auftraggeber die Mittel und Zwecke der Verarbeitung und gerade nicht der Steuerberater. Im Gegensatz hierzu erläuterte das Bayerische Landesamt für Datenschutzaufsicht in seinem Tätigkeitsbericht 2017/2018[4], dass die Beauftragung von Steuerberatern in der Regel nicht als Auftragsverarbeitung zu bewerten sei. Die Aufsichtsbehörde begründet ihre Auffassung mit der weisungsfreien und eigenverantwortlichen Mandatsausübung und dem Hinweis auf die Untersagung der gewerblichen Tätigkeit neben der eigentlichen Steuerberatung (§ 57 Abs. 4 Nr. 1 StBerG). Zudem stützt das Bayerische Landesamt seine Rechtsauffassung auf das bereits genannte Kurzpapier Nr. 13. Interessant an diesen beiden diametral auseinanderliegenden Rechtsauffassungen ist die Tatsache, der unterschiedlichen Bewertung der berufsrechtlichen Vorgaben und deren Einfluss auf die Auftragsverarbeitung.

Berufsrechtliche Aspekte

Das Berufsrecht regelt sowohl den Berufszugang als auch die Berufsausübung. Die Verletzung von Berufspflichten kann zivilrechtliche Auswirkungen (Haftung gegenüber dem Mandanten), wie auch strafrechtliche Auswirkungen (Verletzung von Privatgeheimnissen, § 203 StGB) haben. Die Überwachung der Einhaltung des Standesrechts erfolgt durch die berufsständischen Kammern. Der Vorstand der Steuerberaterkammer kann Berufspflichtverletzungen durch die Erteilung eine Rüge ahnden (§ 82 StBerG). Weitere berufsgerichtlichen Maßnahmen, wie etwa ein zeitlich beschränktes Berufsverbot oder die Ausschließung aus dem Beruf sind möglich (§ 90 StBerG).

Die weisungsfreie Berufsausübung des Steuerberaters sichert seine Vertrauensposition in zweierlei Richtungen ab: Der Mandant kann sich sicher sein, dass der Steuerberater als freier Beruf kein nur verlängerter Arm der Finanzverwaltung ist[5] und die Öffentlichkeit und die Finanzverwaltung können darauf vertrauen, dass der Steuerberater kraft seiner fachlichen Kompetenz Erklärungen und Einschätzungen abgibt und nicht aus Gefälligkeit seinem Mandanten gegenüber. Nicht umsonst ist der Steuerberater neben dem Wirtschaftsprüfer und dem vereidigten Buchprüfer bei der Beantragung der Überbrückungshilfen in Höhe von 24,6 Mrd. Euro für kleine und mittlere Unternehmen[6], die durch die Maßnahmen zur Eindämmung der Corona-Pandemie in Deutschland Umsatzeinbußen hatten, der Vertrauensanker der öffentlichen Verwaltung, wenn es darum geht, Missbrauch und Betrug auszuschließen, wie sie ohne seine Einbindung bei Beantragung der Soforthilfen scheinbar bereits stattfanden[7].

Bewertung berufsrechtlicher Aspekte

Ursächlich für die unterschiedliche Bewertung durch Datenschutzaufsichtsbehörden dürfte auch die differenzierte Bewertung der Tätigkeit des Steuerberaters gewesen sein. Mag auf den ersten – und ausschließlich auf semantische Auslegung gerichteten – Blick das Steuerberatungsgesetz nur die Steuerberatung regeln, umfasst der gesetzlich festgelegte Anwendungsbereich des Steuerberatungsgesetzes bei einer Steuerberatung weit mehr, nämlich nicht nur gemäß § 1 Nr. 1 StBerG Hilfeleistungen „in Angelegenheiten, die durch Bundesrecht, Recht der Europäischen Union oder der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum geregelte Steuern und Vergütungen betreffen, soweit diese durch Bundesfinanzbehörden oder durch Landesfinanzbehörden verwaltet werden“, sondern auch gemäß § 1 Abs. 2 Nr. 2 StBerG „die Hilfeleistung bei der Führung von Büchern und Aufzeichnungen sowie bei der Aufstellung von Abschlüssen, die für die Besteuerung von Bedeutung sind“. Damit zählen Beratungen und Dienstleistungen bei der Lohnbuchführung, also die damit zusammenhängenden Berechnungen, Abführungen, ▶

[3] 34. Tätigkeitsbericht, https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf, Abruf: 06.07.2020, S. 57.

[4] 8. Tätigkeitsbericht 2017/2018, https://www.lda.bayern.de/media/baylda_report_08.pdf, Abruf: 06.07.2020, S.63.

[5] BT Drucksache 3/128 vom 10.01.1958, Entwurf eines Gesetzes die Rechtsverhältnisse der Steuerberater und Steuerbevollmächtigten (Steuerberatungsgesetz), S. 23

[6] https://www.ueberbrueckungshilfe-unternehmen.de/UBH/Navigation/DE/Home/home.html, Abruf 09.07.2020

[7] Vgl. https://www.tagesschau.de/investigativ/ndr-wdr/corona-soforthilfe-betrug-101.html, Abruf 26.07.2020

Deklarationen und Nachweispflichten, zu den Aufgaben, zu denen der Steuerberater nach § 3 StBerG befugt ist. Die Konsequenzen für diese unterschiedlichen Bewertungen waren immens: Mandanten, die den Vorgaben ihrer jeweiligen Datenschutzaufsichtsbehörden folgen und Sanktionen in Millionenhöhe[8] vermeiden wollten, forderten über den Abschluss einer Vereinbarung zur Auftragsverarbeitung das Bekenntnis zu einer weisungsabhängigen Tätigkeit des Steuerberaters, was dessen zuständige Kammer als Verstoß gegen Berufspflichten bewerten würde. Die Steuerberater befanden sich damit in einem Entscheidungskonflikt. Sollten sie der Anforderung des Mandanten, eine Vereinbarung zur Auftragsverarbeitung unterschreiben, wohl wissend, dass dies gleichzeitig zu einem Verstoß gegen das Berufsrecht führt? Die unterschiedlichen Auffassungen der Aufsichtsbehörden förderten diese Diskussion. Auch weitere Aufsichtsbehörden äußerten sich zu dem Themenkomplex: so sprach sich z.B. die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen klar für eine Auftragsverarbeitung bei einer Lohnbuchhaltung durch den Steuerberater aus, auch der Hessische Beauftragte für Datenschutz und Informationsfreiheit schloss eine Auftragsverarbeitung bei dessen Tätigkeitsbereichen nicht aus, während das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) und der Sächsische Datenschutzbeauftragte keine Auftragsverarbeitung annahmen[9].

Übrigens gab es in Österreich bei einer vergleichbaren Ausgangslage bereits 2018 einen Bescheid der dortigen Datenschutzbehörde zur einheitlichen Klärung der Rechtsfrage. Die Wirtschaftstreuhänder (Steuerberater und Wirtschaftsprüfer) unterliegen einer vergleichbaren Berufsregelung wie die deutschen Steuerberater im StBerG, da auch diese als freie Berufe klassifiziert werden (§ 1 Bundesgesetz über die Wirtschaftstreuhandberufe – öWTBG). Die Datenschutzbehörde entschied im Januar 2018, dass Wirtschaftstreuhänder als Verantwortliche („Auftraggeber" nach dem öDSG 2000) anzusehen sind, weil die berufsrechtlichen Regelungen aus § 71 öWTBG zu einer eigenverantwortlichen Berufsausübung einer weisungsgebundenen Tätigkeit auch bei der Lohn- und Gehaltsabrechnung entgegenstehen.[10]

Ohne Gesetzgeber ging es nicht

Der Gesetzgeber sah sich daher gezwungen, gesetzgeberische Klarheit zu schaffen. 2019 gab es zwei unterschiedliche Initiativen im Rahmen von Gesetzgebungsverfahren. Im Dritten Gesetz zur Entlastung insbesondere der mittelständischen Wirtschaft von Bürokratie (Drittes Bürokratieentlastungsgesetz BEG III) empfahlen die Ausschüsse Finanzen, innere Angelegenheiten und Recht des Bundesrates eine Änderung des § 11 Abs. 2 StBerG[11]. Sie wollten eine klarstellende Ergänzung, um die Interpretation einzelner Landesdatenschutzbeauftragten, dass es sich bei den in § 6 Nr. 4 StBerG genannten Tätigkeiten „Buchen laufender Geschäftsvorfälle", „laufende Lohnabrechnung" und „Fertigen der Lohnsteuer-Anmeldungen" nicht um Tätigkeiten der Hilfeleistung in Steuersachen im Sinne von § 1, § 33 StBerG handele, zu korrigieren. Die in § 6 Nr. 4 StBerG genannten Tätigkeiten „Buchen laufender Geschäftsvorfälle", „laufende Lohnabrechnung" und „Fertigen der Lohnsteuer-Anmeldungen" seien gerade nicht vom Anwendungsbereich des Steuerberatungsgesetzes ausgenommen. Denn § 6 StBerG ordne an, dass die genannten Tätigkeiten von dem in § 5 StBerG angeordneten Verbot der unbefugten Hilfeleistung in Steuersachen ausgenommen sind. Diese Ausnahme vom Verbot der unbefugten Hilfeleistung in Steuersachen setze zwingend voraus, dass die in § 6 StBerG genannten Tätigkeiten Hilfeleistungen in Steuersachen im Sinne des StBerG sind. Zudem sei klarzustellen, dass die dem Steuerberater und anderen in § 3 StBerG aufgeführten Personen und Gesellschaften mit der Lohnbuchführung im Sinne von § 34 Steuerberatervergütungsverordnung (StBVV) typischerweise erteilten Aufträge der „Führung der Lohnkonten und Anfertigung der Lohnabrechnungen" (vgl. § 34 Absatz 2 StBVV) Tätigkeiten bzw. Leistungen darstellen, die über die in § 6 Nr. 4 StBerG genannte „laufende Lohnabrechnung und das Fertigen der Lohnsteuer-Anmeldungen" hinausgehen. Die Leistung des mit der Lohnbuchführung beauftragten Steuerberaters umfasse regelmäßig vielmehr die eigenverantwortliche Prüfung und Anwendung der gesetzlichen Bestimmungen.

Parallel dazu hat auch der Deutsche Bundestag im Rahmen des Gesetzgebungsverfahrens zum Jahressteuergesetz (genauer „Gesetz zur weiteren steuerlichen Förderung der Elektromobilität und zur Änderung weiterer steuerlicher Vorschriften") über die

[8] so die damalige Empfindungslage aufgrund unseriöser Marketingaussagen meist auch unseriöser Berater

[9] Siehe mit Fundstellen Kramer/Schmidt, ZD 2020, 194 (197)

[10] GZ: DSB-D122.767/0001-DSB/2018 vom 22. 1.2018; abrufbar unter https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20180122_DSB_D122_767_0001_DSB_2018_00/DSBT_20180122_DSB_D122_767_0001_DSB_2018_00.pdf, Abruf: 26.07.2020

[11] Bundesrat Drs 454/1/19 vom 27.9.2919, Seite 12

Änderungsvorschläge des Finanzausschusses vom 7.11.2019[12] eine Klarstellung angestrebt. Danach erfolgte die Ergänzung in § 11 Abs. 2 S. 1 StBerG, dass die Verarbeitung personenbezogener Daten durch Personen und Gesellschaften nach § 3 StBerG unter Beachtung der für sie geltenden Berufspflichten weisungsfrei erfolgt. Dies gelte auch für das „Buchen laufender Geschäftsvorfälle", „laufende Lohnabrechnung" und „Fertigen der Lohnsteuer-Anmeldungen". Denn die Leistung des mit der Lohnbuchführung beauftragten Steuerberaters umfasst die eigenverantwortliche Prüfung und Anwendung der gesetzlichen Bestimmungen.

Diese Regelung stellt die berufsrechtlichen Pflichten des Steuerberaters als Berufsgeheimnisträger zur unabhängigen, eigenverantwortlichen, gewissenhaften und verschwiegenen Berufsausübung sicher. Zugleich erfolgte mit einer Klarstellung in § 11 Abs. 2 S. 2 StBerG eine Anpassung an die DSGVO, dass auch besondere Kategorien von personenbezogenen Daten in diesem Rahmen gemäß Art. 9 Abs. 2 lit. g DSGVO verarbeitet werden dürfen. Damit wurde auch für die Verarbeitung besonderer Datenkategorien wie etwa von Gesundheitsdaten durch einen Steuerberater eine zweifelsfreie, weil gesetzliche Grundlage geschaffen. Die Ergänzung diene dazu unter Wahrung und Beachtung der besonderen Vertrauensstellung des Steuerberaters die notwendige Rechtssicherheit für alle Beteiligten zu schaffen und so die ordnungsgemäße steuerliche Beratung zu gewährleisten.

Happy End – für alle?

Letztendlich hat sich der Gesetzgeber für die Umsetzung aus dem Jahressteuergesetz entschieden und diese im Bundesgesetzblatt veröffentlicht[13]. Damit ist nun final geklärt, dass der Steuerberater kein Auftragsverarbeiter für seinen Mandanten bei der Erbringung der Lohn- und Gehaltsbuchhaltung sowie der Finanzbuchhaltung ist. Seitdem hat sich die Diskussion beruhigt und die damit verbundene Rechtsunsicherheit für Steuerberater, deren Mandanten und nicht zuletzt auch bei deren datenschutzrechtlichen Beratern wurde beseitigt.

Auch für die deutschen Aufsichtsbehörden lassen sich positive Aspekte erkennen: Der etwaige Aufwand zwecks Beantwortung von Fragen zu diesem Themenbereich entfällt. Zudem wird der aktuellen politische Diskussion um eine Zusammenlegung der Datenschutzaufsichtsbehörden im nicht-öffentlichen Bereich ein plakativer Anwendungsfall durch die Klarstellung in § 11 StBerG entzogen.[14]

Gleichwohl ist festzustellen, dass die uneinheitliche Rechtsanwendung von bundeseinheitlichem Recht durch die verschiedenen Datenschutzaufsichtsbehörden mitunter schwer vermittelbar ist. Selbst der Datenschutzkonferenz, als Gremium der unabhängigen Datenschutzbehörden des Bundes und der Länder mit ihren verschiedenen Arbeitskreisen gelingt es mitunter nicht, eine gemeinsame Basis zu finden, der sich alle Häuser anschließen können oder wollen[15]. Einheitliche und verlässliche Kriterien für die Rechtsanwendung sind gerade in einem komplexen Gebiet wie dem Datenschutzrecht dringend geboten. Wenn ein Unternehmen in mehreren Bundesländern Standorte unterhält oder als Auftragsverarbeiter bundesweit Dienstleistungen anbietet, dann sind die unterschiedlichen Rechtsauffassungen der Aufsichtsbehörden zur Herbeiführung einer unternehmensweiten, einheitlichen Vorgehensweise durch den datenschutzrechtlichen Berater mitunter nur schwerlich vermittelbar und in der Konsequenz undurchführbar. Unüberwindbare Abgrenzungsschwierigkeiten führen zu Unsicherheiten bei der Rechtsanwendung, die so sicherlich auch nicht im Sinne des EU-Verordnungsgebers waren. Die unmittelbare Anwendung der Verordnung wird ad absurdum geführt, wenn in Deutschland höchst unterschiedliche Interpretationsansätze durch die Aufsichtsbehörden vertreten werden.

Über die Autoren

Rudi Kramer
Rechtsanwalt (Syndikusrechtsanwalt), DATEV eG, Stellv. Vorstandsvorsitzender des BvD

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

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

swds
DATENSCHUTZRECHT FÜR UNTERNEHMEN

[12] Bundestag Drs. 19/14909 vom 7.11.2019, S. 58

[13] BGBl. 2019, Teil I Nr. 48, vom 17.12.2019, S. 2451

[14] Vgl. https://www.handelsblatt.com/politik/deutschland/dsgvo-bremsklotz-fuer-digitalwirtschaft-union-will-neuorganisation-der-datenschutzaufsicht/25989768.html, Abruf: 09.07.2020

[15] vgl. hierzu zuletzt: Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail, Orientierungshilfe des Arbeitskreises „technische und organisatorische Datenschutzfragen" vom 13. März 2020

DATENVERARBEITUNG VON DER BEWERBUNG BIS ZUM JOBWECHSEL

Caroline Gigger und Jutta Sonja Oberlin

Einführung

Nirgends im Unternehmen finden sich so viele personenbezogene Daten wie in der Personalabteilung, auch Human Ressources genannt: Vom Namen über Geburtsdatum, von Adresse, über Gehaltsangaben bis zu Daten, welche unter «sensibel» klassifiziert werden. Letztere sind als besondere Kategorien personenbezogener Daten zu verstehen und in der gesetzlichen Terminologie gemäss Art. 9 DSGVO als spezielle Kategorien von Daten bezeichnet. Dazu gehören Daten, die in die sehr private, wenn nicht intime Sphäre eines Individuums fallen. Etwa Angaben zur Religionszugehörigkeit, zur politischen Meinung oder zur Gesundheit. Doch was müssen Unternehmen beachten, um «Human Ressources»-Daten (HR-Daten) sicher zu verarbeiten? Was gilt es datenschutzrechtlich zu beachten? Mithilfe des vorliegenden Beitrags soll ein Grundverständnis rund um die Thematik des Datenschutzes im Beschäftigtenverhältnis geschaffen werden.

Die Datenverarbeitung im Arbeitsverhältnis

Personalabteilungen verarbeiten relevante Informationen eines Angestellten, die sich im Laufe des Arbeitsverhältnisses ansammeln. Dabei geht es oftmals um sensible Angaben, welche der Angestellte als vertraulich behandelt wissen möchte. Sie sollen nur für Zwecke verarbeitet werden, die dem Arbeitsverhältnis dienen.[1] Kein Mitarbeiter wünscht, dass seine Daten ohne Kenntnis und Einwilligung zweckentfremdet an Dritte weitergegeben werden oder bei einem Hackerangriff abgegriffen und womöglich im Darknet verkauft werden. Der Personalabteilung kommt somit grosse Verantwortung zu.

Bei der Verarbeitung von HR-Daten sind die betroffenen Datensubjekte neben den internen oder externen Angestellten auch Bewerber und ausgeschiedene Mitarbeiter. In der Datenschutz-Grundverordnung (DSGVO) werden Datenarten nicht in dem Sinne kategorisiert[2], dass Vorschriften zu etwaigen «Arbeitnehmerdaten» vorzufinden sind. Vielmehr definiert Art. 4 Nr. 1 DSGVO personenbezogenen Daten als solche, «die sich auf eine identifizierte oder identifizierbare natürliche 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». Dazu zählen allgemeine Kontaktdaten wie Name, Adresse, Telefonnummer oder andere Personalien wie Geburtsdatum, Staatsangehörigkeit, Zivilstand und Geschlecht. Auch etwaige Legitimationsdaten wie Pass- oder Ausweisnummern, Steuer- und Kontonummern sowie Informationen über die Bonität des Bewerbers kommen in Betracht.

[1] Unter die Bezeichnung Arbeitsverhältnis wird auch bspw. die Bewerbungsphase, sowie auch die Zeit der Nachabwicklung eines einstigen Arbeitsverhältnisses subsumiert

[2] Ausnahme: Spezielle Kategorien von Daten gemäss Art. 9 DSGVO

In den HR-Akten werden auch fortlaufende Angaben zum Arbeitsverhältnis an sich festgehalten, etwa Daten aus dem Performance-Management hinsichtlich des persönlichen beruflichen Fortkommens, dem Learning-Management oder den Zielvereinbarungen innerhalb eines Geschäftsjahres. Daneben werden auch Daten gemäss Art. 9 (1) DSGVO verarbeitet. Dabei geht es um jene Daten, «aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten». Auch biometrischen Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person dürfen demnach nicht erhoben werden. Dieses Verbot ist jedoch «nur» ein Verbot mit Erlaubnistatbeständen und so darf beispielsweise gemäss Art.9 (1) DSGVO die Verarbeitung durch eine rechtsgültige Einwilligung stattfinden.

Zur Datenerhebung im Beschäftigungsverhältnis gilt im Allgemeinen in der Schweiz und in Deutschland, dass der Arbeitnehmer die Privatsphäre des Arbeitnehmers zu beachten hat.[3] In Deutschland lassen sich noch spezifische datenschutzrechtliche Bestimmungen in verschiedenen Gesetzen verorten, etwa in § 39 Abs. 8 Einkommensteuergesetz oder § 18 f Sozialgesetzbuch (SGB) Viertes Buch (IV) sowie im kollektiven Arbeitsrecht § 75 (2) BetrVG. In der DSGVO lässt die Vorschrift des Art. 88 (1) DSGVO den Mitgliedstaaten Freiraum, durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung und zur Erfüllung des Arbeitsvertrags zu erlassen. Aus deutscher Sicht ist § 26 BDSG zur «Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses» ausschlaggebend.

Lebenszyklus der Daten:

Um sich einen Überblick über die erhobenen Daten zu verschaffen, sollte ein Blick auf die verschiedenen Etappen des Lebenszyklus der Daten geworfen werden. Ein solcher Zyklus beinhaltet das Verfahren von der Bewerbung bis zum Ausscheiden des Arbeitnehmers aus dem Unternehmen. Vorab ist zu erwähnen, dass bei der Datenverarbeitung im gesamten Zyklus stets die Datenschutzprinzipien auch im Rahmen eines Arbeitsverhältnisses gelten. Dazu zählen nach Art. 5 DSGVO die Rechtmässigkeit (Verarbeitung nach Treu und Glauben/Transparenz), die Zweckbindung, die Datenminimierung, die Richtigkeit, die Speicherbegrenzung, die Integrität und Vertraulichkeit und die Rechenschaftspflicht. Bei sorgfältiger Umsetzung ist der Grundstein des datenschutzkonformen Umgangs gelegt.

Um der Rechenschaftspflicht[4] nachzukommen, sollte die Verarbeitung dokumentiert und technische und organisatorische Massnahmen angepasst werden. Mittels eines Verzeichnisses von Verarbeitungstätigkeiten[5] kann einfach und übersichtlich eine gute Basis für die Dokumentation gelegt werden. Es wird geraten, dass auch Unternehmen unter 250 Mitarbeitern dieses führen sollten.[6]

Bewerbungsverfahren

Es gibt zahlreiche Möglichkeiten, als Bewerber in das Bewerbungsverfahren zu gelangen. Gewöhnlich geschieht dies durch Initiativbewerbung oder durch das Bewerben auf eine Stellenanzeige. Der Bewerber schickt in der Regel ein Motivationsschreiben, seinen Lebenslauf und seine Zeugnisse. Darin gibt er auf Verlangen des potenziellen Arbeitgebers Auskunft über personenbezogene Daten aller Art[7], welche von allgemeinen Kontaktdaten bis hin zu Geburtsdatum, Staatsangehörigkeit, Zivilstand und Geschlecht reichen. Dazu kommen die oben bereits ausgeführten Daten. Des Weiteren können durch extracurriculare Aktivitäten weitere Daten im Sinne von Art. 9 DSGVO hinzukommen.

Der Grundsatz der Verhältnismässigkeit aus Art. 5 DSGVO gebietet seitens des Arbeitgebers, dass stets nur Angaben eingefordert werden, welche auch erforderlich sind für das zu begründende Arbeitsverhältnis. Dies gilt auch für Fragen zu einer Schwangerschaft bei einem Bewerbungsgespräch. Wenn diese nicht für die zu besetzende Stelle von absoluter Relevanz ist - etwa für eine gefährliche oder beschwerliche Arbeit - muss der Arbeitgeber sich damit abfinden, dass die betroffene Person keine Angaben macht. Dies darf beim nachträglichen Entdecken der Schwangerschaft auch nicht zu einer Anfechtung des Arbeitsverhältnisses führen.[8] Zudem darf diese Frage aus rechtlicher Perspektive ohnehin nicht gestellt werden, da sie das im Gleichstellungsgesetz verankerte Diskriminierungs- ▶

[3] Siehe Art. 328 (1) und Art. 328 b des Obligationenrechts (OR) für die Schweiz

[4] Art. 5 (2) DSGVO

[5] Art. 30 DSGVO

[6] So gemäss Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 10

[7] Gemäss Art. 4 DSGVO

[8] Siehe das altbekannte Beispiel nach der Schwangerschaftsfrage Bundesarbeitsgericht Urt. v. 15.10.1992, Az.: 2 AZR, 227/92; oder BAG, Urteil v. 6. 2.2003 – 2 AZR 621/01

verbot verletzt. Nur solche Fragen, welche für die Entscheidungsfindung wichtig sind, dürfen gemäss des Grundsatzes der Datenminimierung aus Art. 5 (1) lit. c DSGVO gestellt werden.[9] Arbeitgebern ist es nur gestattet personenbezogene Daten zu sammeln und zu erheben soweit es für die angestrebte Position erforderlich ist.[10] Bei der Stellenausschreibung empfiehlt der Schweizer Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), dass der Arbeitgeber sich vor der Ausschreibung einer vakanten Stelle über die mitzubringenden Qualifikationen und das Anforderungsprofil ein präzises Bild von den gewünschten Anforderungen macht. Bewerberinformationen sollten nicht nach Belieben erfragt werden, um erst im Nachhinein zu entscheiden, welche dieser Angaben tatsächlich benötigt werden.[11]

Bei der Benutzung von cloudbasierten HR-Anwendungen ist zudem zu berücksichtigen, dass Daten grenzüberschreitend übermittelt werden können. Dagegen spricht auch nichts, solange das Land gemäss Art. 4 DSGVO ein angemessenes Datenschutzniveau gewährleistet oder geeignete Garantien getroffen wurden. Für große Unternehmen mit einer ausgereiften Datenschutzstruktur eignen sich zudem gemäss Art. 47 DSGVO die verbindlichen internen Datenschutzvorschriften. Die Daten, welche an den Empfänger gelangen, sollten dabei nur auf das erforderliche Maß einsehbar sein.[12] Hier sei angemerkt, dass seit dem EuGH-Urteil vom 16.07.2020 (Schrems II, C-3111/18) gilt, dass das „Privacy Shield" nicht mehr als zulässiger Mechanismus eingesetzt werden darf, um personenbezogene Daten von der EU in die USA zu übermitteln.[13] Dieser bahnbrechende Entscheid stellt die USA jenen Ländern gleich, welche ausserhalb der EU/EWR oder nicht in einem Kommissionsbeschluss als Land mit einem datenschutzrechtlich angemessenen Schutzniveau bezeichnet wurden.

Was das Löschen angeht, sollte auf Fristen geachtet werden: Will ein Bewerber eine Benachteiligung wegen eines vom Allgemeinen Gleichbehandlungsgesetz (AGG) verbotenen Merkmals geltend machen, muss er dies innerhalb einer Frist von zwei Monaten[14] tun. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) hält eine Speicherung von Bewerbungsunterlagen nach Abschluss des Auswahlverfahrens über vier Monate hinaus für nicht erforderlich. Er empfiehlt Arbeitgebern, nach Ablauf dieser Zeitspanne eine Löschung zu veranlassen.[15] Sollten Profile in ein Bewerberpool zur Besetzung neuer Stellen aufgenommen werden, ist eine Einwilligung des Betroffenen erforderlich.[16] Dabei sollten die Datenschutzhinweise konkret formuliert werden. Hierbei ist insbesondere auf die jederzeitige Widerrufsmöglichkeit der Einwilligung hinzuweisen.[17]

Im laufenden Arbeitsverhältnis

Ist der Bewerber erfolgreich in das Arbeitsverhältnis eingetreten, hinterlässt er im Arbeitsalltag Datenspuren. Bei vielen Unternehmen wird bei Arbeitsbeginn und Arbeitsende die Zeit erfasst. Per Mail und über andere digitale Kommunikationswege findet ein permanenter Austausch statt, Fotos werden erstellt oder Social-Media-Kanäle bedient. Zudem sammelt die HR-Abteilung wichtige Daten im Personaldossier. Darunter fallen Personalien und Adressdaten, Bewerbungsunterlagen, Referenzauskünfte, der Arbeitsvertrag und Entgelte, Angaben über Arbeitsausfälle, Krankheiten und Arztzeugnisse, Lohn- und Versicherungsdaten, Angaben zum Performance Management oder mögliche Disziplinarmassnahmen wie Verwarnungen, Verweise oder Bußgelder. Der Schweizer EDÖB empfiehlt hier, dass das Personaldossier einer regelmässigen Selektion -in der Regel jedes zweite Jahr- unterzogen werden sollte und die in dem Rahmen nicht mehr benötigten Unterlagen entfernt werden.[18]

Die Einwilligung

Eine Besonderheit im Rahmen des Arbeitsverhältnisses stellt die Verarbeitung aufgrund der Einwilligung dar, wenn die gesetzlichen Erlaubnistatbestände nach Art. 6 (1) lit. b bis f DSGVO nicht greifen. Erwägungsgrund 42 DSGVO schreibt zur Einwilligung gemäss Art. 7 DSGVO vor, dass nur dann davon ausgegangen werden sollte, dass eine Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine «echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden». Gemäss Erwägungsgrund 43 sollte «in besonderen Fällen, wenn zwischen

[9] Vgl. Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 24

[10] Opinion 2/2017 on data processing at work, Adopted on June 2017 WP 249, S. 11

[11] Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 27

[12] Opinion 2/2017 on data processing at work, Adopted on June 2017 WP 249, S. 22

[13] Urteil des EuGH vom 16. Juli 2020, Rechtssache C-311/18.

[14] § 15 (4) AGG

[15] Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 32

[16] Bergt, in: S.810 Koreng/Lachenmann 2. Auflage 2018 H I 1

[17] Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 33

[18] Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich Bearbeitung durch private Personen, Stand Oktober 2014 des Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, S. 12

der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern».

Im Rahmen des Beschäftigtenverhältnisses stellt sich also die Frage nach der Freiwilligkeit einer durch den Angestellten abgegebenen Willenserklärung: Wie freiwillig ist eine Einwilligung in Anbetracht des Abhängigkeitsverhältnisses, welches ein Arbeitsverhältnis mit sich bringt? Dieses Problem bezieht sich dem Grunde nach auf alle Arten von Abhängigkeitsverhältnissen.[19] Das Vorliegen einer Freiwilligkeit wird oftmals als problematisch angesehen, da die wirtschaftliche und persönliche Abhängigkeit des Arbeitnehmers suggeriert, dass die Person in einer Zwangslage steckt und somit nicht frei entscheiden kann. Arbeitnehmer seien selten in der Lage tatsächlich freiwillig einzuwilligen.[20] Dies bestätigt auch das LfDI Baden-Württemberg, wonach es in der Praxis an der notwendigen Freiwilligkeit der Einwilligung fehle.[21] Eine abgegebene Einwilligung kann aber nur dann wirksam sein, wenn der Arbeitnehmer die Möglichkeit hat, selber zu bestimmen, ob und wie seine Daten verwendet werden können. Dazu gehört auch, dass er ohne Furcht vor möglichen Konsequenzen seine Einwilligung jederzeit entziehen kann.[22]

Für die Einwilligung im Rahmen des Beschäftigungsverhältnisses gelten somit spezielle Anforderungen: Der Betroffene muss hinreichend bestimmt und transparent über die konkrete Tragweite seiner Entscheidung aufgeklärt werden. Erfolgt die Einwilligung via schriftlicher Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen der Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache derart erfolgen, dass von anderen Sachverhalten klar zu unterscheiden ist.[23] Erwägungsgrund 32 fügt hinzu, dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen sollte, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (etwa in Form einer schriftlichen oder einer mündlichen Erklärung). Erstere kann auch elektronisch erfolgen.

Die Einwilligung ist dem LfDI Baden-Württemberg nach, in Konstellationen möglich, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen. Etwa bei der Erlaubnis, den Dienstwagen nicht nur für berufliche, sondern auch für private Zwecke zu nutzen, der Arbeitgeber dem Arbeitnehmer das Diensthandy und andere EDV-Geräte zum privaten Gebrauch überlässt oder wenn der Arbeitnehmer seinen Namen auf eine Geburtstagsliste setzen lässt.

Die Verarbeitung personenbezogener Daten von Beschäftigten sei im Grunde oft zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich und könne deshalb auf § 26 BDSG als gesetzliche Grundlage gestützt werden.[24] Somit muss und sollte erst gar nicht das Gewicht primär auf die Einwilligung gelegt werden, solange es um essentielle Sachverhalte zum Arbeitsverhältnis geht. Wenn eine Einwilligung doch zum Zuge kommt, hat der deutsche Gesetzgeber mit § 26 (2) S.2 BDSG normiert, dass erst dann eine sogenannte Freiwilligkeit vorliegen kann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Weitere technische Massnahmen des Arbeitgebers

Im Arbeitsverhältnis fallen unter Umständen auch Daten durch Tracking und Monitoring an. Das Aushändigen von Laptops, Handys und Tablets ermöglicht ein mobiles Arbeiten im Auto, im Zug oder von Zuhause. Von letztere Option sind durch Covid 19 viele Arbeitnehmer betroffen und haben ihren Arbeitsort ins Homeoffice verlegt. Der Arbeitnehmer gewinnt damit an Flexibilität und Freiheit, zugleich möchte der Arbeitgeber die Geräte vor Hackerangriffen und Malware schützen. Dazu gehört mitunter auch eine physische Ortung der Geräte. Besonders in Handwerksberufen ist es üblich, dass GPS-Ortungs- und Trackingfunktionen in Mobilgeräten, Laptops oder in Autos eingebaut werden. Zudem ist es weit verbreitet, dass das Bedürfnis des Arbeitgebers besteht, Mobilgeräte und Laptops nachzuverfolgen, falls diese abhandenkommen.

In diesem Rahmen wird auch in die Privatsphäre des Arbeitnehmers eingegriffen. Der Arbeitgeber wird dies gemäss Art. 6 (1) lit. d DSGVO mit der ▶

[19] Bergt, in: S.804 Koreng/Lachenmann 2. Auflage 2018 H I 1

[20] Opinion 2/2017 on data processing at work, Adopted on June 2017 WP 249, S. 4

[21] Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 20

[22] Erwägungsgrund 42; Bergt, in: S. 804 Koreng/Lachenmann 2. Auflage 2018 H I 1

[23] Art. 7 (2) DSGVO

[24] Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 20; im gleichen Sinne auch WP249 Opinion 2/2017 on data processing at work, Adopted on 8 June 2017, S. 4

Wahrung der berechtigten Interessen rechtfertigen und dies zweckdienlich unter den Aspekt der Sicherheit subsumieren. Dabei sollte der Arbeitgeber stets die Möglichkeit wählen, welche für das Datensubjekt am wenigsten invasiv ist (Prinzip der Verhältnismässigkeit).[25] Dadurch lässt sich ein missbräuchliches Überwachen des Arbeitnehmers vermeiden. Zu erinnern ist dabei stets an den Lidl-Überwachungsskandal 2008, bei dem der Discounter in die Negativschlagzeilen geriet. Dies zeigt, dass viele Compliance-Risiken nicht «nur» Sanktions-Risiken beinhalten, sondern auch ein Reputationsrisiko.

Um dies zu vermeiden, sollte das Augenmerk auf Art. 25 DSGVO und Art. 35 DSGVO gelegt werden («data protection by design and by default» und «data protection impact assessments»). Datenschutz muss danach eine Schlüsselkomponente bereits bei der Festlegung des Mittels – etwa einer Applikation- sein. «Data Protection by default» hingegen legt die Pflicht fest, angemessene technische und organisatorische Massnahmen zu treffen zum Wohle der Datensparsamkeit sowie «privacy-freundliche» Features.[26]

Es ist sinnvoll, im Vorhinein in einer Richtlinie festzulegen, über welche Zwecke Protokolldaten wann und von wem abgerufen werden können. Daran können sich die Angestellten orientieren, um sie über eine akzeptable und inakzeptable Nutzung des Netzes zu informieren. Dies ermöglicht es, dass das Nutzerverhalten so angepasst werden kann, dass eine Überwachung überflüssig wird.[27]

Mailzugriff bei unvorhersehbaren Abwesenheiten

Eine gegenwärtige Frage, welche aber noch nicht geregelt ist, stellt der Mailzugriff bei unvorhergesehenen Abwesenheiten des Arbeitnehmers dar. Dies betrifft Abwesenheiten beispielsweise bei Krankheiten oder Unfällen, die den Arbeitnehmer ad hoc über einen längeren Zeitraum daran hindern, seiner geschäftlichen Tätigkeit nachzugehen. Unter Umständen ist es nötig, auf die Mails des Betroffenen zuzugreifen, mit der Gefahr, dass dabei auch private Nachrichten eingesehen werden. Die Frage wird unterschiedlich gehandhabt. Einige Arbeitnehmer untersagen gänzlich den privaten Mailverkehr über die Arbeits-E-Mail-Adresse, während andere ihn hingegen gewähren. Der einfachste aber zugleich radikalste Weg, sich abzusichern, wäre eine vollständige Untersagung der Privatnutzung. Weniger drastische Alternativen stellen das Ernennen eines Stellvertreters dar, der Zugriff auf die Mails hat, oder eine automatische Weiterleitung der Mails an denselben. Beides birgt aber wieder das Risiko, dass private Nachrichten mitgelesen werden könnten.

Welcher Weg auch gegangen wird, es ist wichtig, dass im Vorfeld das Einverständnis des Mitarbeiters unter Darlegung des Zwecks schriftlich eingeholt wird. Wenn daraufhin der Zugriff auf das Postfach erfolgt, darf keinesfalls eine Mail, welche offensichtlich privater Natur ist (etwa im Betreff als «Privat» gekennzeichnet), durch den Arbeitgeber verarbeitet werden. Um unliebsame Überraschungen zu vermeiden, sollte dieser Umgang in einem firmeninternen Reglement festgehalten werden, damit der Arbeitnehmer weiss, wie bei unerwarteter Abwesenheit mit seinen Mails umgegangen wird. So können sich sowohl Arbeitnehmer als auch Arbeitgeber auf ihre Rechte und Pflichten einstellen.[28] Auf diese Weise wird dem Transparenzgebot nachgekommen. Dies entschied auch der Europäischen Gerichtshofs für Menschenrechte (EGMR) bei einem Überwachungssachverhalt, wonach die Internetkommunikation der Beschäftigten überwacht werden dürfe, sofern die Arbeitnehmer vorab über die Möglichkeit allfälliger Überwachungsmassnahmen informiert werden.[29] Die Entscheidung unterstreicht, dass bei Zugriffen auf das Postfach stets der vorherigen Informationspflicht nachgekommen werden sollte.

Auflösung des Arbeitsverhältnisses

Grundsätzlich ist es geboten, die Daten nach Beendigung des Arbeitsverhältnisses aufgrund des Zweckentfalls[30] oder gemäss des Grundsatzes der Datenminimierung zu löschen - es sei denn es gelten gesetzlich vorgeschriebene Aufbewahrungspflichten. Persönliche Daten wie Eignungstests, Qualifikationsberichte und psychologische Tests, die nicht mehr zweckdienlich sind und somit nicht mehr den Anforderungen aus Art. 5 Abs. 1 lit. c DSGVO genügen, sind umgehend zu vernichten.

[25] Opinion 2/2017 on data processing at work, Adopted on June 2017 WP 249, S. 13.

[26] Eva Irene Wille, in: Rücker/Kugler, New European General Data Protection Regulation A Practioner's Guide, 2018, Rn 1159.

[27] Opinion 2/2017 on data processing at work, Adopted on June 2017 WP 249, S. 14.

[28] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Zugriff auf Mailbox bei Kündigung oder Krankheit (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/arbeitsbereich/zugriffauf-e-mail.html)

[29] Urt. Vom 5.07.2017, Bărbulescu gegen Rumänien, Beschwerde Nr. 61496/08.

Etwas anderes gilt bei Daten, die aufgrund einer gesetzlichen Pflicht aufbewahrt werden müssen oder bei denen, deren Aufbewahrung im Interesse der Angestellten liegt. Im Regelfall sollten aufbewahrungspflichtige Daten mit einer Frist von fünf Jahren gespeichert werden, die – wenn das Gesetz dies vorsieht – auf zehn Jahre verlängert werden kann.[31] Dafür sollten klare Löschkonzepte eingeführt werden, um der Speicherbegrenzung nach Art. 5 (1) lit. e DSGVO nachzukommen.[32] Ein solches Löschkonzept stellt durch technische und organisatorische Massnahmen sicher, dass nach Beendigung der rechtskonformen Datenverarbeitungsaktivität die Löschung der Daten auch tatsächlich erfolgt.[33]

Wichtig ist, dass bei der Verarbeitung im gesamten Zyklus, gegen externe als auch gegen interne Gefahren, technische und organisatorische Massnahmen gem. Art. 32 DSGVO ergriffen werden, um ein angemessenes Schutzniveau zu gewährleisten. Dies ist ein elementarer Schritt, damit es nicht zu einer unbefugten Einsichtnahme, unzulässigen Verarbeitung oder sonstigen «Datenpanne» gemäss Art. 4 Nr. 12 DSGVO kommt. Es ist essenziell, dass passende Zugriffsberechtigungen etabliert sind oder dass die Kommunikation verschlüsselt erfolgt. Es empfiehlt sich, Identity and Access Management-Lösungen wie Zeitzertifikate einzurichten, um sicherzustellen, dass kein Unberechtigter Zugriff auf die Daten hat. Die DSGVO stärkt die Betroffenenrechte und verpflichtet die Verantwortlichen zur umfassenden Auskunftserteilung, welche dem Angestellten zustehen. Unternehmen sollten sich also nicht nur auf vermehrte Anfragen von Kunden, sondern auch auf Fragen der eigenen Mitarbeiter einstellen.

Fazit

Die Datenverarbeitung im Arbeitsverhältnis ist durch viele Besonderheiten geprägt. Als Faustregel kann gesagt werden, dass sich bei jedem Vorhaben die allgemeinen Datenschutzprinzipien wie ein roter Faden durch die Verarbeitungsaktivitäten ziehen sollten. Diese bieten jedem Verarbeiter einen zuverlässigen Anhaltspunkt. Wenn sie richtig angewendet werden, verringert man das Risiko einer unrechtmässigen Datenverarbeitung. Als Arbeitgeber gilt es darauf zu achten, dass dies im Rahmen der Verhältnismässigkeit vonstatten geht. Wenn tatsächlich auf die Erhebung mittels Einsatzes einer bestimmten Massnahme nicht verzichtet werden kann und dafür ein legitimer Grund vorliegt, sollte man besonders auf die Datensparsamkeit achten. Nur wenn das Vorhaben tatsächlich erforderlich ist für den jeweiligen angestrebten Zweck und keine alternativen, milderen Möglichkeiten ersichtlich sind, sollte die Massnahme ergriffen werden. Es ist davon auszugehen, dass in näherer Zukunft mehr behördliche Informationen zum Thema Beschäftigtendatenschutz verfügbar sind.

Über die Autorinnen

Caroline Gigger

ist Senior Consultant im Cybersecurity Team bei der PricewaterhouseCoopers AG in Zürich. Sie gehört dem Team Data Protection and Regulatory Compliance an und berät Kunden aus verschiedenen Industrien zu datenschutzrechtlichen Themen mit Schwerpunkt DSGVO.

Jutta Sonja Oberlin

CIPP/E, CIPM, ist zertifizierte Datenschutzbeauftragte und zertifizierte Compliance Officer (Univ.) Bei PWC in Zürich ist sie als Unternehmensberaterin im Bereich Regulatory Compliance tätig und berät Kunden zu aller Art von datenschutzrechtlichen Sachverhalten. Durch ihren rechtlichen Ausbildungshintergrund ist es Ihr möglich als Schnittstelle zwischen rechtlichen und technischen Gegebenheiten zu fungieren. Zudem ist sie Mitglied der IAPP Leadership Community und engagiert sich in der Schweiz als Young Privacy Professional Lead.

[30] https://www.handelskammerjournal.ch/de/das-recht-auf-vergessen-herausforderung-implementierungsgigant-oder-doch-nicht-so-heiss-gegessen-wie-gekocht

[31] Leitfaden für die Bearbeitung von Personendaten im Arbeitsbereich Bearbeitung durch private Personen, Stand Oktober 2014 des Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB, S. 14

[32] https://www.handelskammerjournal.ch/de/das-recht-auf-vergessen-herausforderung-implementierungsgigant-oder-doch-nicht-so-heiss-gegessen-wie-gekocht

[33] Ratgeber zum Beschäftigtendatenschutz – 4. Auflage, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, April 2020, S. 53

„CORONA KAM FÜR UNS ETWAS ZU FRÜH."

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Stefan Brink, im Interview mit den BvD-News.

Die Datenschutzaufsichtsbehörde in Baden-Württemberg war von dem Shutdown in der Hochphase der Corona-Pandemie in Deutschland hart getroffen. Komplexe Datenverarbeitung und Datensicherheit erlaubten erst nach und nach, mehr Mitarbeiterinnen und Mitarbeiter ins Homeoffice zu schicken. Nun blickt das Team um den Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, nach vorn. Über den Digitalisierungsschub, die nächsten Schritte der Aufsichtsbehörde und die Arbeit im Lockdown sprachen die BvD-News mit Stefan Brink.

BvD-News: *Herr Brink, wie steht es nach dem Digitalisierungsschub im Zuge des Corona-Lockdown um den Datenschutz?*

Brink: Wir werden schauen müssen, in welchen Bereichen Datenschutz nachgeholt werden muss. Das reicht von einzelnen Branchen bis hin zu Fragen, die alle betreffen, zum Beispiel, wie die Verbindung zu Video-Konferenzsystemen sicher wird. Sich allein an der DSGVO zu orientieren, bot während des Shutdowns mitunter keine Lösung. Zwar gibt es Videoanbieter, die alle Anforderungen der Ende-zu-Ende-Verschlüsselung einhalten. Manchmal sind diese Verbindungen aber instabil oder haben Schwierigkeiten mit der Übertragungsbandbreite.

BvD-News: *Wie wollen Sie Aufklärung betreiben?*

Brink: Zum einen wollen wir sicherstellen, dass auch weiterhin stabile Video-Konferenzen möglich sind. Zum anderen wollen wir darüber informieren, wie die Nutzerinnen und Nutzer selbst die Verbindungen sicherer gestalten können. Und natürlich beraten wir auch Betriebe und Behörden, wie sie die Verbindungen in Homeoffices DSGVO-sicher machen können.

BvD-News: *Industrie- und Unternehmensverbände plädierten bereits dafür, den Datenschutz im Zuge der Pandemie zu lockern. Wie bewerten Sie diese Haltung?*

Brink: Das ist schon fast ein Reflex bei den Interessenvertretungen der Industrie. Aber die DSGVO gilt natürlich weiterhin. Wir sind zwar in der Praxis aktuell noch verständnisvoll, wenn ein Unternehmen durch den Lockdown erst nach und nach datenschutzrechtlich sichere Verbindungen zu den Mitarbeiterinnen und Mitarbeitern zuhause einrichten kann. Aber bei klaren Rechtsverstößen gilt der Bußgeldkatalog der DSGVO auch weiterhin. Daran ändert Corona nichts.

BvD-News: *Wir arbeiten Sie und Ihre Mitarbeitenden denn derzeit?*

Brink: Ich hoffe, dass wir in den nächsten Wochen wieder stärker vor Ort sein können. Während des Lockdowns war es ja für uns nicht möglich, Betriebe aufzusuchen und auf Dienstreise zu gehen. Da war die Kontrolltätigkeit doch sehr runtergefahren.

BvD-News: *Wie haben Sie und Ihr Team überhaupt während der strengen Kontaktbegrenzungen gearbeitet?*

Brink: Corona kam für uns etwas zu früh. Wir konnten zum Zeitpunkt des Shutdowns zunächst erst rund ein Drittel der Belegschaft sicher und verschlüsselt von zu Hause aus arbeiten lassen. Diejenigen, die nicht zur Risikogruppe gehörten, mussten in Abständen in die Behörde kommen und Akten austauschen. Als Aufsichtsbehörde müssen wir ja hohe Sicherheitsstandards bei der Datenverarbeitung, der Datensicherheit und Verschlüsselung erfüllen. Das ist zeitaufwändig und kostenintensiv. Zudem haben wir für die Verschlüsselung keine Tokens mehr bekommen. Das war nicht anders mit Headsets. Es hat uns also erst mal schwer getroffen.

Aber schließlich haben wir es geschafft, für zwei Drittel des Teams einen Heim-Arbeitsplatz einzurichten. Ein weiteres Drittel musste in der Behörde bleiben, Techniker zum Beispiel, die Kollegen aus der Personalverwaltung oder unsere Hausmeister.

BvD-News: *Gab es noch weitere Änderungen?*

Brink: Corona hat vor allem die Eingänge bei Beschwerden grundlegend verändert. Beschwerden gegenüber der Wirtschaft sind deutlich zurückgegangen. Das ist zumindest für jene Meldungen plausibel, die aus dem Kontext von Handel und Dienstleistungen stammen. Denn die Geschäfte hatten geschlossen, viele Dienstleistungen wurden, wo möglich, virtuell angeboten. Im öffentlichen Sektor gab es jedoch einen deutlichen Anstieg an Beschwerden.

BvD-News: *Was waren das für Beschwerden?*

Brink: Zum einen betraf es die Umsetzung von Erlassen und Richtlinien der Gesundheitsministerien von Bund und Ländern. Da hatten viele Bedenken, was sich auch in der Zahl der Beschwerden zeigte. Es betraf aber auch Fragen zum Verhalten der Polizei, etwa ab wann die Beamten bei vermeintlichen Verstöße gegen die Kontaktbeschränkungen die Personalien aufnehmen durften. Außerdem gab es viel mehr Nachfragen zum Beschäftigtendatenschutz, zum Beispiel die Frage, ob ein Arbeitgeber das Ergebnis eines Corona-Tests einfordern kann oder ob jemand für die Arbeit vom Homeoffice aus sein privates Handy nutzen muss. Aber auch viele Gastwirte meldeten sich, weil sie nicht wussten, wie sie mit den Personendaten umgehen sollten, die sie derzeit aufnehmen müssen, um etwaige Infektionsketten nachvollziehbar zu machen. Oder ob sie die eingetragenen Namen und Adressen kontrollieren dürfen.

BvD-News: *Das sind eigentlich Fragen, die den generellen Umgang mit den Corona-Anforderungen betreffen und nicht so sehr Datenschutzfragen allein, oder?*

Brink: Absolut. Da hätten Bund und Länder mehr Informationen bereitstellen müssen. Wir haben dann zum Beispiel für Gastwirte Musterformulare erarbeitet und Informationen gegeben, wie sie die Listen nach Ablauf der Aufbewahrungsfrist sicher vernichten.

Das Interview führte BvD-Redakteurin Christina Denz

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

▶ www.baden-wuerttemberg.datenschutz.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Über die Autorin

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

FULL HOUSE ONLINE

Rund 800 Teilnehmende bei der ersten virtuellen Video-Ausgabe der BvD-Verbandstage

Karsten Füllhaase

Als die Corona-Pandemie Deutschland im März vollends erreichte, war die Verunsicherung zunächst groß. Wie wird sich die Lage weiterentwickeln? Wie lange wird das öffentliche Leben stillstehen? In mehreren Sondersitzungen beschäftigte sich der BvD-Vorstand damals mit der Frage, welche Auswirkungen die Pandemie auf den BvD haben wird, und wie darauf zu reagieren ist. Im Zentrum dieser Diskussionen standen immer auch die BvD-Verbandstage Anfang Mai, sind diese doch eines der Großereignisse der Jahres – nicht nur für die Mitglieder.

Schon damals begannen parallel die Planungen für eine digitale Variante, sollte das Verbot von Großveranstaltungen bis Mai aufrechterhalten werden. Als dann klar wurde, dass das Branchentreffen nicht wie gewohnt im Ellington Hotel in Berlin stattfinden kann, ging alles ganz schnell: Das Programm wurde an die Anforderungen der digitalen Welt angepasst, die nötige IT-Infrastruktur geprüft und bereitgestellt, und schon wurden die Einladungen verschickt für die ersten „BvD-Verbandstage online". Mit der großen Resonanz, die auf diese Einladung folgte, hatte wohl niemand gerechnet: Rund 800 Teilnehmer nahmen vom 4. bis zum 7. Mai 2020 an insgesamt zwölf Online-Webinaren und -Seminaren teil. Auf besonderes Interesse stießen die beiden vom BvD-Vorstandsvorsitzenden Thomas Spaeing moderierten Gesprächsrunden unter dem vieldeutigen Motto „Datenschutz in der Krise?" zu den besonderen Herausforderungen im Datenschutz in Zeiten von Corona: Zum Auftakt mit Prof. Ulrich Kelber, Bundesbeauftragter für Datenschutz und Informationsfreiheit, und zum Abschluss mit Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Ulrich Kelber plädierte im Zusammenhang mit den derzeit populären Videokonferenz-Tools zur Eröffnung der BvD-Verbandstage für mehr europäische und zertifizierte Produkte, die Prinzipien wie Privacy by Design und Privacy by Default folgen würden. Die großen fünf Anbieter auf dem Markt hätten noch immer datenschutzrechtliche Probleme. Sichere und datenschutzkonforme Anbieter seien zwar kostenpflichtig, aber unterm Strich „allemal billiger als Dienstreisen".

Brink berichtete zum Abschluss der Verbandstage, dass er in seiner Behörde derzeit einen deutlichen Rückgang bei Beschwerden im privaten Bereich beobachten würde, im Gegenzug aber die Beschwerden im öffentlichen Sektor – etwa über Polizei, Ordnungs- und Gesundheitsämter – stark zugenommen hätten. Mit Blick auf die Zeit nach Corona nannte Brink „Aufräumen" als Hauptaufgabe der Aufsichtsbehörde: „Wir müssen dafür sorgen, dass Datenbestände, die jetzt gesammelt werden, nach der Krise rückstandsfrei gelöscht werden. Da werden wir auch in Dokumentationen von Behörden genau sehen wollen, was wann gelöscht wurde." (Ein Interview mit Dr. Stefan Brink finden Sie auf S. 72 in dieser Ausgabe)

Auch ein Thema, das aktuell wieder heiß diskutiert wird, streifte Brink bereits im Mai: die Gespräche in Berlin, um die Zuständigkeiten für die Aufsicht über die Unternehmen beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zusammenzuführen. Das Thema ist nicht neu, so wurden Ideen in dieser Richtung schon seit Längerem vereinzelt diskutiert, zuletzt im vergangenen Jahr sowohl von Vertretern der SPD als auch der CDU. Der Bund wäre für die Schaffung einer einzelnen Aufsichtsbehörde für die Unternehmensseite nicht auf die Zustimmung der Länder angewiesen. „Wir haben die Pfeile schon gespitzt", äußerte sich Brink zu der erneut aufkeimenden Debatte. Gerade für kleine und mittlere Unternehmen sei durch die Zuständigkeit der Datenschutz-Aufsichtsbehörden auf Länderebene eine bessere Nähe und Erreichbarkeit gegeben, als dies bei einer zentralen Aufsicht der Fall wäre.

Neben den kostenlosen Auftakt- und Abschlussgesprächen gab es täglich einstündige Webinare und umfassende Online-Seminare. Als Referenten waren zu hören: Lars Hillen (Konzerndatenschutzbeauftragter der Debeka-Gruppe), Dr. Jens Eckhardt (Derra, Meyer & Partner Rechtsanwälte PartGmbB), Bonni Silverman (Referentin der Berliner Beauftragten für Datenschutz und Informationsfreiheit), Stefan Sander (SDS Rechtsanwälte Sander Schöning), Thomas Kahl (Taylor Wessing Partnerschaftsgesellschaft mbB), Maria-Christina Rost (Persönliche Referentin des Hessischen Datenschutzbeauftragten), Andreas Sachs (Vizepräsident des Bayerischen Landesamtes für Datenschutzaufsicht), Regina Mühlich (AdOrga Solutions GmbH), Barbara Thiel (Landesbeauftragte für Datenschutz Niedersachsen) und Andrea Backer-Heuveldop (ds² Unternehmensberatung GmbH & Co. KG).

Nicht nur die BvD-Verbandstage fanden erstmals online statt. Auch die in ihrem Rahmen üblicherweise festlich begangene Verleihung des Datenschutz Medienpreises (DAME) des BvD wurde in den virtuellen Raum verlegt (Einen Bericht zum „Unboxing" der Preispakete und der digitalen Preisverleihung finden Sie ebenfalls in dieser Ausgabe auf Seite 76).

„Wir freuen uns, dass unsere erste Online-Ausgabe der BvD-Verbandstage so positiv aufgenommen worden ist und erfolgreich war", sagte Thomas Spaeing. „Auch wenn der informelle persönliche Austausch am Rande einer physischen Konferenz im virtuellen Raum nicht abgebildet werden konnte, fühlen wir uns bestärkt, in dieser Richtung weiterzudenken.

Über die Autoren

Karsten Füllhaase
ist seit Januar 2020 Leiter des BvD-Hauptstadtbüros. Neben der Leitung und Betreuung der Geschäftsstelle begleitet er vor allem die Entwicklung des europäischen Dachverbands EFDPO und unterstützt den Vorstand bei der Ausschussarbeit sowie der politischen Verbandskommunikation in Berlin. Der Kulturwissenschaftler ist Kommunikationsprofi mit 15-jähriger Erfahrung in leitenden Positionen für Stiftungen und gemeinnützige Gesellschaften.

Regina Mühlich
ist Geschäftsführerin der AdOrga Solutions GmbH; Datenschutzbeauftragte, Datenschutz-Auditorin, Compliance Officer, anerk. Sachverständige für Informationsverarbeitung und Datenschutz, zert. Informationssicherheitsbeauftragte ISO/IEC 27001 (ISMS), BvD-Vorstandsmitglied.

▶ www.AdOrgaSolutions.de

Neue Erfahrungen nicht nur für Dozenten

BvD-Vorstandsmitglied Regina Mühlich.

Erstmals in der Geschichte des BvD wurden die Verbandtage als reine Online-Veranstaltung durchgeführt. 800 Teilnehmerinnen und Teilnehmer hatten sich für die virtuellen Vorträge und Online-Seminare angemeldet – ein absoluter Rekord. So viele Teilnehmer hätten in den Konferenzsaal des Ellington-Hotels in Berlin niemals gepasst. Alle geplanten Formate wurden vom BvD entsprechend angepasst.

Das Online-Format brachte neue Erfahrungen für die 800 Teilnehmerinnen und Teilnehmer, aber auch für die Dozenten. Im Gegensatz zu vielen anderen Online-Veranstaltungen, wo Diskussionen und Fragerunden eher verhalten ausfallen, war dies beim BvD-Online-Verbandstag erfreulich anders. Die gute Laune und das Engagement der Teilnehmerinnen und Teilnehmer war zu spüren. Es gab rege Diskussionen und eine aktive Teilnahme in den Webinaren und den fast fünfstündigen Online-Seminaren. Von kleinen Hängern in der Videoübertragung abgesehen, hat der Austausch in den Veranstaltungen gut funktioniert.

Für die Dozenten ist eine Online-Veranstaltung eine deutlich größere Herausforderung. Es fehlt großenteils das direkte Feedback aus dem Publikum. Darüber hinaus ist der Blick auf teilweise leere Teilnehmericons ohne Bildübertragung nicht gerade motivierend. Der persönliche Austausch zwischen den Vorträgen, in den Pausen, bei einem Kaffee, beim Mittagessen oder abends bei einem Glas Wein, fehlte sowohl den Dozenten, den Teilnehmern als auch dem BvD-Vorstand. Es gab keine begleitenden Gespräche zu den Vortrags- und Seminarthemen. Dies lässt sich im Online-Vortragsrahmen nicht abbilden. Im klassischen Rahmenprogramm wird argumentiert, neue Projektideen kreiert oder Partnerschaften gebildet. In diesen freien Diskussionsrunden kam seinerzeit auch die Idee für die Herbstkonferenz zustande, die bereits drei Mal alternierend in Stuttgart und Nürnberg stattfand. Wir hoffen also, dass wir uns vom 14. bis 16. Oktober 2020 wieder „live" und diesmal in Mannheim sehen können.

Online Vorträge, Seminare und Webinare für Datenschutzbeauftragte anzubieten wird aber auch über Corona hinaus eine gute zusätzliche Alternative sein. Mittlerweile haben sich viele mit den Online-Formaten angefreundet und es entfallen Reisekosten und Reisezeit. Wer viel unterwegs ist, weiß es zu schätzen, sich von einem anderen Ort „mal schnell" in eine Online-Veranstaltung einzuklinken. Der BvD lädt daher für das 2. Halbjahr 2020, neben den Präsenzveranstaltungen, auch zu diversen Online-Veranstaltungen und Seminaren ein. Aber das physische Treffen mit Kollegen und Bekannten, mit Fachleuten und Gleichgesinnten ist am Ende doch durch Nichts zu ersetzen. Kurzum – wir danken für Ihr Engagement und Interesse und freuen uns auf Ihre Teilnahme – online und live vor Ort.

UNBOXING STATT GLITTERKANONE

Die DAME-Preisverleihung fand in diesem Jahr online statt

Christina Denz

„Also damit hätte ich jetzt echt nicht gerechnet." YouTuber Felix Michels ist sichtlich aus dem Häuschen, als er das BvD-Paket öffnet, das ihm die Post gerade zugestellt hat. Aus dem Paket holt Michels zuerst die große Glückwunschkarte, dann den Symbolcheck über 3.000 Euro und schließlich die transparente DAME-Trophäe, den Datenschutz Medienpreis 2019.

„Coole Sache."

Felix Michels ist der diesjährige Gewinner der DAME, die der BvD bereits zum dritten Mal an Medienproduktionen vergab, die Datenschutz verständlich, anschaulich und mit Blick auf ihre Zielgruppe ansprechend vermitteln. Michels erhielt die Auszeichnung für sein Video „Das weiß das Internet über Dich! – Selbstexperiment". „Krass", sagt Michels über seinen Gewinn. „Coole Sache."

Dass es in diesem Jahr ein Paket per Post statt einer Gala im Rahmen der BvD-Verbandstage in Berlin, dass es ein „Unboxing" statt einer Glitterkanone wie bei den vergangenen Preisverleihungen gab, dafür waren die Kontaktbeschränkungen im Rahmen der Corona-Pandemie verantwortlich. Deshalb verlegte der BvD nicht nur seine Verbandstage ins Internet, sondern auch die diesjährige DAME-Preisverleihung.

Paketpost vom BvD erhielten auch die beiden anderen Nominierten, Jakob Leube und Freddy Radeke, für ihren „Xtra3"-Satire-Beitrag „Facebook in Real Life" sowie Christian Schiffer für die Hörfunkreportage „Tracking: Ein Tag im Internet – welche Spuren hinterlasse ich."

„Keiner der drei Nominierten wusste, wer den Preis erhält", berichtet DAME-Projektkoordinatorin Katrin Eggert. „Wir haben nur alle drei gebeten, das ‚Unboxing' zu filmen." Zur Begründung gab das DAME-Team an, dass die Videos, die die Nominierten beim Auspacken aufnehmen sollten, zwar für die Preisverleihung sei, aber nur in einem Paket der Hauptpreis sei. Entsprechend groß war die Überraschung bei den anderen Nominierten, als sie ihre Pakete öffneten und darin ebenfalls einen Preis fanden.

„Wie ein warmer Pullover, der nicht kratzt."

Christian Schiffer beobachtet in seinem Hörfunkbeitrag „Tracking: Ein Tag im Internet – welche Spuren hinterlasse ich" sein eigenes Internet-Verhalten mit Fitnessarmband, beim Online-Shopping, bei Downloads oder beim Liken auf Social-Media-Kanälen. Witz und Selbstironie gepaart mit Informationen, was mit unseren Daten im Internet passiert, überzeugte die Jury – und vergab den Kategoriepreis „Bester Beitrag Hörfunk".

Aber davon weiß Schiffer noch nichts, als er das BvD-Paket erhält. Für ihn ist es „das erste ‚Unboxing'-Video, dass ich in meinem ganzen Leben aufgezeichnet habe", sagt er, kramt im Paket und holt die Gewinnerbenachrichtigung heraus. „Das finde ich toll, das freut mich sehr", sagt er, vor allem „dass das Thema ein bisschen die Prominenz bekommt, die es verdient" begeistert ihn an dem Preis. Aber auch die Trophäe selbst gefällt Schiffer. „Sie ist schön leicht und transparent, so wie es ja auch im Internet und beim Datenschutz sein sollte, also transparente Regeln und eine gewisse Leichtigkeit, damit der Datenschutz so implementiert wird, dass ihn die Menschen gar nicht merken, dass er ihnen gar nicht mehr auffällt, dass es Datenschutz by design gibt". Insgesamt fühlt sich der Preis für ihn an „wie ein warmer Pullover, der nicht kratzt".

„Wie beim Champions-League-Pokal."

Jakob Leube hat seinen Teamkollegen Freddy Radeke per Videokonferenz mit ins Bild geschaltet, als er das Paket öffnet. „Ich bin total aufgeregt. Das ist doch spannend", sagt Radeke und schaut zu, wie Leube die Klebebanderole aufreißt. Dann kommt die Gewinnerkarte zum Vorschein für „Bester Beitrag Comedy und Satire", der Symbolcheck über 1.500 Euro und der Preis selbst mit der Gravur der beiden Gewinner.

„Ein Preis: Ich raste aus, ich werd nicht mehr. Da ist wirklich ein richtiger Preis drin", freut sich Leube. Und beim Lesen der Gravur auf der DAME-Trophäe gerät er ins Schwärmen: „Wie beim Champions-League-Pokal." Er habe noch nie einen Preis mit Preisgeld gewonnen, „außer von der örtlichen Sparkasse bei einen Malwettbewerb".

Radeke, der das „Unboxing" per Video verfolgt, ist ebenfalls begeistert: „Wir freuen uns tierisch, dass wir unseren ersten gemeinsamen Preis haben."

Beide hätten die Satire, die in drei Szenen Social-Media-Verhalten ins echte Leben überträgt und damit zeigt, wie leichtfertig die Nutzer Daten preisgeben, nur machen können, weil sie sich selbst so verhielten. Erst durch den Film hätten sie eigene Verhaltensmuster hinterfragt. „Das war eine Art Selbsttherapie", sagt Radeke. Einziger Wehrmutstropfen für Leube: Dass es in diesem Jahr keine Live-Veranstaltung gab, „sonst hätten wir jetzt schön anstoßen können".

Das wird im nächsten Jahr nachgeholt. Die Gewinner aus diesem Jahr werden bei der großen Verleihungsgala im Rahmen der BvD-Verbandstage 2021 mit auf der Bühne sein.

Die Preisverleihung

BvD-Vorstandsvorsitzender Thomas Spaeing war bislang Co-Moderator neben Ralph Caspers bei DAME-Preisgalas im Rahmen der BvD-Verbandstage in Berlin. In diesem Jahr erfolgte die Preisverleihung virtuell und auf YouTube. Ein Auszug aus Thomas Spaeings Eröffnungsrede:

„33 Einreichungen, Kinofilme, dokumentarische, Clips und Erklärfilme, Radiobeiträge sowie Webvideos und ganze Webseiten mit vielen Clips über Datenschutz hatten sich um die DAME 2019 beworben. Die Einreichungen haben wieder gezeigt: Datenschutz muss gar nicht trocken sein. Datenschutz erklären kann sogar witzig, geistreich, emotional und aufregend sein, vor allem aber verständlich. Das war unser Ziel: Das wir Beiträge fördern, die Datenschutz verständlich machen. Anschaulich, praktisch und Lösungen für Datenschutz im Alltag anbieten.

Wie auch bei den ersten beiden Ausschreibungen hatten wir in der Jury wieder viel Spaß beim Sichten der Beiträge. Datenschutz kann wirklich witzig sein. Aber wir hatten auch Diskussionen: Zählen Emotionen mehr als Aufklärung? Viele Beiträge schaffen beides und die haben uns besonders gefallen. Die Entscheidung war dennoch nicht leicht. Deshalb auch ein herzliches Dankeschön an die Vorjahresgewinner Gion Hunziger, Meret Kaufmann und Nicolas Zürcher. Die Medienstudenten aus der Schweiz hatten mit dem Kurzfilm „Chancen und Risiken von Gesundheitsdaten" die DAME 2018 gewonnen."

Die Jury 2019

Birgit Kimmel – Päd. Leitung klicksafe.de, Landeszentrale für Medien und Kommunikation (LMK)

Klaus Müller – Vorstand des Verbraucherzentrale Bundesverbands (vzbv)

Frederick Richter – Vorstand Stiftung Datenschutz

Thomas Spaeing – Vorstandsvorsitzender des BvD

Barbara Thiel – Landesbeauftragte für den Datenschutz Niedersachsen

Stefanie Rack – Referentin der EU-Initiative klicksafe

Dr. Sebastian Sprenger – Referent der DATEV-Stiftung Zukunft

Die DAME-Gewinner 2018, **Meret Kaufmann, Gion Hunziker** und **Nicolas Zürcher**, gaben ebenfalls ihr Votum ab. Der Datenschutz Medienpreis (DAME) wird seit November 2018 von der DATEV-Stiftung Zukunft gefördert.

Die Gewinner-Beiträge können Sie direkt über den QR-Code auf der BvD-Internetseite abrufen

Über die Autorin

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

Aus der Begründung der Jury …

… für den Gewinner der DAME 2019, Felix Michels

Barbara Thiel:

> *Felix Michels zeigt auf sehr frische und gleichzeitig verständliche Art, welche Dimensionen das Sammeln von Daten durch das Internet angenommen hat. Er legt außerdem gezielt den Finger in die Wunde vieler Userinnen und User: Denn einen beträchtlichen Teil der über uns zugänglichen Daten haben wir selbst preisgegeben. Felix Michels macht so – ohne belehrend zu wirken – auf Risiken und Missbrauchsmöglichkeiten aufmerksam. Damit leistet er einen wichtigen Beitrag zur Aufklärung über die Bedeutung des Datenschutzes. Zusätzliche Tiefe erhält sein Video durch die Einbeziehung eines Experten von netzpolitik.org.*

Sebastian Sprenger:

> *Felix Michels ist mit über 500.000 YouTube-Abonnenten ein Sprachrohr für die heutige Jugend und schafft es mit seiner Reportage, wertvolle Aufklärungsarbeit zu leisten. Arbeit, die bei den Jugendlichen ankommt!*

… für den „Besten Beitrag Hörfunk" von Christian Schiffer

Stefanie Rack:

> *Der Beitrag ist sehr abwechselungsreich, sehr witzig und durch die Experteninterviews super interessant. Jeder Zuhörer kann sich an irgendeinem Punkt eigentlich wiederfinden.*

Barbara Thiel:

> *Christian Schiffer macht mit seinem Radiobeitrag deutlich, dass ein vollkommener Verzicht auf Online-Teilhabe heutzutage an der Realität vorbei geht. Das Problem ist nicht, dass jeder von uns Daten produziert. Das Problem ist vielmehr, dass diese Daten von Unternehmen verknüpft, ausgewertet und wirtschaftlich ausgeschlachtet werden, ohne dass wir darauf immer Einfluss nehmen können. Hier ist die Politik gefragt, Regeln zu erlassen und durchzusetzen.*

… für den „Besten Beitrag Humor und Satire" von Jakob Leube und Freddy Radeke

Klaus Müller:

> *Die Autoren machen uns durch ihre Überzeichnung deutlich, wie wertvoll meine Daten sind und wie peinlich es eigentlich ist, wenn wir andere an privaten Daten teilhaben lassen. Und das zeigen sie auf wirklich witzige und spannende Weise.*

Frederick Richter:

> *Die Methode ist einfach und bestechend: Hier wird nichts digitalisiert, sondern analogisiert. Denn das Verhalten vieler im Netz, der Selbstexhibition persönlichster Details in der Öffentlichkeit wird hier schön veranschaulichst in einer Art Hofnarretei des Datenschutzes.*

Anzeige

25% Rabatt auf den Jahrespreis für BvD Mitglieder

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

https://www.datenschutz-berater.de

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

Per Faxantwort an 069/7595-1150

Name: _____

Firma: _____

Abteilung: _____

Straße: _____

PLZ | Ort: _____

Telefon: _____

E-Mail: _____

Datum | Unterschrift: _____

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

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

Sie erhalten die nächsten 3 Ausgaben der Fachzeitschrift „Datenschutz-Berater" kostenlos. Falls Ihnen der „Datenschutz-Berater" gefällt, brauchen Sie nichts weiter zu unternehmen. Wenn Sie nicht innerhalb der Testzeit abbestellen, beginnt im Anschluss ein Jahresabo. Zunächst für ein Jahr (11 Ausgaben) zum Vorzugspreis von derzeit 324,26 € abzgl. 25% Rabatt für BvD Mitglieder inkl. aller Gebühren und reduzierter MwSt. in Deutschland und anschließend bis auf Widerruf zum jeweils gültigen Jahrespreis abzgl. 25%. Das Abonnement kann bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar.

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

Sie erhalten die nächsten 11 Ausgaben der Fachzeitschrift „Datenschutz-Berater", sowie den Zugang zur Online-Datenbank. Der Abonnementvertrag wird für mindestens ein Jahr abgeschlossen. Das Abonnement kann jederzeit bis 3 Monate vor Ablauf des Bezugszeitraumes schriftlich bei der Deutscher Fachverlag GmbH, Mainzer Landstr. 251, 60326 Frankfurt am Main gekündigt werden. Liegt dem Verlag zu diesem Zeitpunkt keine Abbestellung vor, verlängert sich das Abonnement automatisch um ein weiteres Jahr. Die Abonnementgebühren sind im Voraus nach Erhalt der Rechnung zahlbar und betragen 324,26 € abzgl. 25% Rabatt für BvD Mitglieder inkl. aller Gebühren und reduzierter MwSt. in Deutschland.

DATENSCHUTZ-BERATER
kundenservice@ruw.de

dfv Mediengruppe

DATENSCHUTZ & MARKETING

Wie Sie Recht und Praxis partnerschaftlich zusammenbringen
Dr. Jens Eckhardt

Dr. Jens Eckhardt
»Datenschutz & Marketing – Wie Sie Recht und Praxis partnerschaftlich zusammenbringen«
PrivacyXperts – Fachverlag für Beratung im Bereich Datenschutz und IT-Security ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG

1. Auflage, 2019
135 Seiten, geb.
139,05 Euro
ISBN: 978-3-8125-2792-7

Zielgerichtete Werbung ist sowohl für das Unternehmen als auch für den Werbeempfänger interessanter. Die am Adressaten ausgerichtete Werbung wirft aber auch Datenschutzfragen auf. Zwischen adressbezogenem Marketing und Datenschutz entsteht ein Spannungsverhältnis. Eine genaue Betrachtung der DSGVO in Bezug u. a. auf Zulässigkeit, Spielräume und Vereinfachungen ist erforderlich. Darüber hinaus geht es um Transparenz- und Dokumentationspflichten.

Das Inhaltsverzeichnis umfasst fünf Seiten und ist umfassend strukturiert:

1. Vorwort Personalisierte Werbung: Nur Datenschutz- oder Wettbewerbsrecht
2. DSGVO: Ist alles anders als davor?
3. Wann Sie beim personalisierten Marketing das Datenschutzrecht beachten müssen und was das bedeutet!
4. Datenschutzaufsichtsbehörden „Orientierungshilfe Direktwerbung“
5. Beachten Sie das Wettbewerbsrecht im Rahmen von Direktwerbung
6. So verlieren Sie nicht den Überblick über die verschiedenen Regelungen im Datenschutzrecht
7. So können Sie ohne Einwilligung des Adressaten Direktwerbung versenden
8. Bereitstellung von Daten durch Dritte zur Neukundengewinnung
9. Das müssen Sie bei der Gestaltung einer Einwilligung in Direktwerbung beachten
10. Das müssen Sie über Big Data, Data Driven Marketing, Targeting & Co. wissen
11. ePrivacy – diese Besonderheiten zum Online-marketing müssen Sie beachten
12. Datenschutzkonforme Einbindung von Dienstleistern und Drittländern

Im Bereich Marketing sind sowohl das UWG (Gesetz gegen unlauteren Wettbewerb) wie auch die DSGVO zu beachten. Beide Rechtsgebiete sind gleichgestellt und es gibt Überschneidungen. Das TKG (Telekommunikationsgesetz) wird ebenfalls einfach und pragmatisch in Zusammenhang gesetzt. Diese Trennung und/oder Gemeinsamkeiten sind gut und leicht verständlich herausgearbeitet. Abgerundet wird die Betrachtung durch gut verständliche Erläuterungen und Kommentierungen des juristischen Kontexts.

Kapitel 4 beleuchtet das personalisierte Marketing und seine datenschutzrechtlichen Implikationen, insbesondere die Zulässigkeit (bzw. Unzulässigkeit) und die Zweckbindung sowie die Informationspflichten (Artt. 13, 14 DSGVO). Die abgedruckten Checklisten sind hilfreich für „habe ich an alles gedacht?" wie auch als Grundlage für die Dokumentationspflichten (Art. 5 Abs. 2 DSGVO).

Die Direktwerbung wird in mehreren Kapiteln des Ratgebers aus Datenschutzsicht bewertet: Zum einen in Kapitel 6 im Zusammenhang mit dem Wettbewerbsrecht und Kapitel 8 im Kontext „Einwilligungen". Nicht zuletzt in Kapitel 10 mit hilfreichen Hinweisen zur Gestaltung von Einwilligungen in der Werbung.

Der Ratgeber wird durch zahlreiche Praxis-Tipps, „Wichtig für Sie" und Anwendungshinweise abgerundet. Zum besseren Verständnis wurde an diversen Stellen „für alte Hasen" ein Vergleich zum BDSG a.F. gezogen. Das Nachschlagewerk erscheint auf den ersten Blick etwas ungewohnt. Es „hangelt" sich nicht wie andere Lehrbücher durch die Artikel des Gesetzes, sondern erläutert Schritt für Schritt sowie schlüssig. Es ist praxisbezogen aufgebaut. Hilfreich sind auch die kurzen Zusammenfassungen, Fallstrickhinweise sowie Empfehlungen für diverse Prüfschritte.

Fazit

Der Ratgeber ist sowohl für erfahrene Praktiker geeignet wie auch für den Anfänger. Dem einen dient es als Nachschlagwerk und Gegenprüfung, dem anderen zum Einlesen und Vertrautmachen mit der Marketingmaterie im Datenschutzrecht.

Die Kapitel des Ratgebers beinhalten ausführliche und hilfreiche Checklisten sowie Prüfungsempfehlungen. Ein Stichwortverzeichnis würde die Suche und das Finden vereinfachen.

Der praxiserprobte Autor hat eine gute Balance zwischen Theorie und Praxis, Tipps und Wissen gefunden.

Ein rundum gut gelungenes und empfehlenswertes Handbuch, welches eine kompetente Unterstützung für Datenschutzbeauftragte bei der Umsetzung der Transparenz- und Dokumentationsanforderungen der DSGVO gibt.

Rezension von

Regina Mühlich
ist Geschäftsführerin der AdOrga Solutions GmbH, Datenschutzbeauftragte, Datenschutz-Auditorin, Compliance Officer, anerk. Sachverständige für Informationsverarbeitung und Datenschutz, zert. Informationssicherheitsbeauftragte ISO/IEC 27001 (ISMS), BvD-Vorstandsmitglied.

▶ www.AdOrgaSolutions.de

RECHTSHANDBUCH CYBER-SECURITY

Tobias Heinrich, Alexander Kiefner, Detlev Gabel (Hrsg.)

Gabel, Heinrich, Kiefer (Hrsg.)
»Rechtshandbuch Cyber-Security«

Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft.

1. Auflage 2019
510 Seiten, Softcover
98,00 Euro
ISBN: 978-3-8005-0012-3

Mit der zunehmenden Digitalisierung der Gesellschaft gewinnt die Absicherung von Systemen und Verbindungen der Informationsverarbeitung immer mehr an Bedeutung. Das früher stiefmütterlich behandelte Thema wird mittlerweile in eigenen Studiengängen gelehrt und Material zur „Cyber-Security" füllt längst viele Regalmeter. Auch der Gesetzgeber hat an vielen Stellen den Einfluss und die Folgen von Sicherheitspannen auf die Gesellschaft und den Einzelnen erkannt und macht zahlreiche Vorgaben zur IT- und Informationssicherheit, die ihr Schattendasein als Anhängsel des Datenschutzes verlassen hat.

Gleich zwei jüngst erschienene Werke unternehmen den Versuch, die die nicht immer konsistenten und nicht selten redundanten Regelungen zu erfassen. Das hier behandelte, von Gabel, Heinrich und Kiefner herausgegebene „Rechtshandbuch Cyber-Security" ist zwar ein wenig preisgünstiger als das von Kipker herausgegebene „Cybersecurity Rechtshandbuch", muss sich aber anders als der Reiseführer „Per Anhalter durch die Galaxis" aus Douglas Adams' Werk deshalb keinesfalls vorwerfen lassen, wie dieser gegenüber der großen „Encyclopaedia Galactica" viele Lücken zu haben und viele Dinge zu enthalten, die sehr zweifelhaft oder zumindest wahnsinnig ungenau sind. Das Gegenteil ist der Fall. Wie beim Anhalter in großen, freundlichen Buchstaben die Worte KEINE PANIK auf den Umschlag zu schreiben, würde den Autoren ebenso aus guten Gründen nicht einfallen.

Schon im Vorwort zitieren sie den Trump-Sondermittler Robert Mueller aus seiner Zeit als FBI-Chef, „es gäbe nur zwei Arten von Unternehmen: Solche, die gehackt wurden und solche, die noch gehackt werden". Als mit dem Thema seit Jahren beschäftigter Leser möchte man hinzusetzen „… oder solche, die noch nicht bemerkt haben, dass sie gehackt wurden". Aus der Erkenntnis heraus, dass jedes Unternehmen betroffen war oder jederzeit sein kann, ergibt sich eine gelungene Struktur, die sich fortan durch das Buch zieht. Für jeden Regelungsbereich wird dargestellt, welche Vorsorgemaßnahmen rechtlich geboten sind (Preparedness) und wie mit einer Sicherheitspanne rechtskonform umzugehen ist (Response). Ergänzt um eine jeweilige Einführung, oft die Darlegung von Kollisionen mit anderen Rechtsgebieten und meist resultierende Haftungs- und Sanktionsregime ergeben sich vier oder fünf Abschnitte für jedes der behandelten Themen, namentlich Gesellschaftsrecht, M&A, Datenschutz, IT-Sicherheit, Arbeitsrecht, Aufsichtsrecht, Kartellrecht, Vergaberecht, Prozessrecht, Strafrecht und Versicherungsrecht. Wo einschlägig, gehen die Autorinnen und Autoren auch auf Spezialgesetze wie z.B. für Banken, Telekommunikationsanbieter oder Atomanlagenbetreiber ein. Solche Vorgaben sind

vielleicht nicht für jedes Unternehmen anwendbar, zeigen jedoch auf, welche Maßnahmen vom Gesetzgeber als wie anspruchsvoll eingeordnet werden.

Im Anschluss an die Darstellung der deutschen (und teilweise europäischen) Rechtslage werden auf mehr als 80 Seiten drei „Länderberichte" in englischer Sprache geliefert, in denen die Grundzüge des jeweiligen Landesrechts in den Bereichen Cyber-Security und Datenschutz für die Vereinigten Staaten, das Vereinigte Königreich und China dargelegt werden. Während Großbritannien durch den laufenden Brexit gesondert zu betrachten ist, werden mit den USA und China große Absatz- und Lieferantenmärkte in den Blick genommen, die insbesondere Beachtung verdienen, weil sie die großen Anbieter von ständig an Bedeutung gewinnenden Cloud-Technologien beherbergen. Der Blick über den Tellerrand ist deshalb sehr bereichernd. Wo es sinnvoll oder nötig ist, wird schon zuvor Bezug auf die Regelungen im Ausland und internationale Entwicklung genommen, zum Beispiel beim Straf- und Prozessrecht.

Im letzten Kapitel werden auf knapp 25 Seiten Checklisten geliefert, die getrennt nach Preparedness und Response als Extrakt der früheren Kapitel auflisten, was zu erfüllen oder zu prüfen ist. Für Datenschützerinnen und Datenschützer ist das Buch insbesondere wertvoll, weil zahlreiche Sicherheitsmaßnahmen Auswirkungen auf die informationelle Selbstbestimmung von Beschäftigten und anderen IT-Nutzerinnen und Nutzern haben. Die erläuterten rechtlichen Anforderungen können entsprechend für Rechtsgrundlagen, Abwägungen und ggf. für Datenschutzfolgenabschätzungen herangezogen werden.

Was das Buch nicht leisten kann, aber wohl auch nicht leisten will, ist konkret technische Einzelmaßnahmen zu empfehlen oder zu bewerten. Daher kann der Titel „Rechtshandbuch" nicht oft genug betont werden. Das Werk ist als Begleitung zu sehen für eine individuelle Sicherheitsarchitektur, für welche die Einhaltung einschlägiger Normen geprüft werden soll. Insbesondere durch die angefügten Checklisten gelingt das sehr gut, sei es als Vollständigkeitskontrolle im Rahmen der Konzeption oder als Prüfleitfaden bestehender Systeme. Dabei sollte niemals vergessen werden, dass eine Prüfung solcher Aspekte trotz guter Impulse und Ausstrahlungswirkungen formaler Natur bleibt. Eine tatsächliche Sicherheit ergibt sich daraus nicht automatisch, womit sich der Kreis zum eingangs zitierten Statement von Robert Mueller schließt.

INFORMATIONSSICHERHEIT UND DATENSCHUTZ

Secorvo Security Consulting (Hrsg.)

Secorvo Security Consulting (Hrsg.)
»Informationssicherheit und Datenschutz«

Handbuch für Praktiker und Begleitbuch zum T.I.S.P. dpunkt. verlag

3. aktualisierte und erweiterte Auflage 2019
824 Seiten, Hardcover
84,90 Euro
ISBN: 978-3-86490-596-4

In der 3., aktualisierten und erweiterten Auflage erscheinen die bisherigen „Zentrale[n] Bausteine der Informationssicherheit" unter dem neuen Titel „Informationssicherheit und Datenschutz". Wie schon in den ersten beiden Auflagen wird das Buch als Begleitbuch zum TeleTrusT Information Security Professional (T.I.S.P.) beworben. Der T.I.S.P. nimmt für sich in Anspruch, ein deutsches Pendant zu den im angelsächsischen Bereich weit verbreiteten Personenzertifizierungen zur IT- bzw. Informationssicherheit zu sein. Er entspricht insoweit am ehesten dem CISSP und das vorliegende Werk einem „Common Body of Knowledge" oder, um mit den Worten der herausgebenden Secorvo Security Consulting – einem Beratungsunternehmen und T.I.S.P.-Schulungsanbieter – zu sprechen, einem „Grundkanon an Basiswissen". Der Vorsatz, das nötige Wissen für eine Umsetzung der Informationssicherheit zusammenzufassen, ist dabei so begrüßenswert wie mutig.

Warum jedoch der Titel in dieser Auflage geändert wurde, bleibt rätselhaft. Während die Informationssicherheit in jedem Kapitel intensiv betrachtet wird, kommt dem Datenschutz über weite Strecken nur eine Statistenrolle zu. Ausführungen zu Rechtsgrundlagen, Betroffenenrechten und Datenpannen sind bestenfalls lückenhaft, Hinweise zu Folgenabschätzungen sucht man vergeblich. Die Ausführungen zum Datenschutz sind im Wesentlichen darauf konzentriert, aus den Artikeln 24, 25 und 32 DSGVO die Notwendigkeit für die Informationssicherheit abzuleiten. Der Datenschutz findet sonst nur Erwähnung, wenn er Werkzeugen der Informationssicherheit Grenzen setzt, so z.B. bei Datensicherung und Archivierung, beim Logging oder der Videoüberwachung.

Im Titel jedoch so zu tun, als würden Informationssicherheit und Datenschutz hier paritätisch erläutert, erscheint unpassend. Es wirkt leider ein wenig so, als wenn die 2018 initiierte Überarbeitung auf der DSGVO-Welle mitreiten wollte. Was nach einem Makel klingt, erweist sich jedoch als Glücksfall für Datenschützerinnen und Datenschützer, deren Vorbildung in den Bereichen Jura oder allgemeiner IT liegt und die sich nun Hintergrundwissen im Bereich Informationssicherheit aneignen möchten. Dafür eignet sich das Buch sehr gut.

Auf mehr als 800 Seiten widmen sich die 14 Autoren in 27 einzelnen Kapiteln jeweils Aspekten der Informationssicherheit und orientieren sich dabei am

T.I.S.P.-Curriculum, ohne sich auf eine Prüfungsvorbereitung einzuengen. Auch wenn die Kapitel laut Kladdentext aufeinander aufbauen, sind sie tatsächlich weitgehend unabhängig voneinander. Im Vergleich zu anderen Büchern, die entweder IT- und Mathematik-lastig sind oder sich auf das Managementtechniken konzentrieren, deckt das vorliegende Werk beides ab und betrachtet zudem Aspekte wie die physische Sicherheit oder Awareness-Maßnahmen. Diese fehlen in vielen anderen Büchern, sind jedoch für umfassende Sicherheitskonzepte gleichwohl wichtig.

Wenig zu beanstanden gibt es auch an der Aktualität des Werkes aus dem Jahr 2019. Gegenüber der zweiten Auflage wurden die Inhalte zum neu verfassten BSI-Grundschutz überarbeitet und ein Kapitel zur Sicherheit von mobilen Endgeräten hinzugefügt. Dass der Gesetzgeber nach Redaktionsschluss des Buches die Mitarbeiterzahl zur Benennung eines Datenschutzbeauftragten herauf gesetzt hat, kann man den Autorinnen und Autoren nicht ankreiden. Wie bei der Breite des Inhalts nicht anders möglich, konzentrieren und beschränken sich die Ausführungen auf Grundlagen und Konzepte, ohne sich zum Beispiel bei Firewalls in Herstellerlisten oder bei der Kryptografie in mathematischen Hintergründen zu verlieren. Die schon beim Datenschutz angemerkte vermeintliche Oberflächlichkeit zieht sich so durch alle Kapitel und das ist positiv zu verstehen. Die fachliche Tiefe entspricht nämlich weitgehend dem, was zum Beispiel in Vertragsanlagen zur Auftragsverarbeitung erwartet wird. Alles weitere hätte den Umfang des Buches sicher gesprengt.

Äußerst angenehm fällt auf, dass die Inhalte durchweg von Autorinnen und Autoren erstellt wurden, die weniger aus akademischer Sicht und Literaturauswertungen heraus argumentieren, sondern bei denen man die praktische Erfahrung aus jeder Seite hinauslesen kann. Die einheitlichen gelungenen grafischen Darstellungen lassen dabei vergessen, dass die Kapitel von verschiedenen Personen verfasst wurden.

Die letzten gut 100 Seiten des Buches runden den Inhalt mit einer Übersicht gängiger Standards, einem Schlagwortverzeichnis und einem Glossar und Abkürzungsverzeichnis ab. Zwar macht sich hier noch einmal bemerkbar, dass das Buch lediglich auf den Zug „Datenschutz“ aufspringt. So fehlen in der Liste der Standards nicht nur das SDM und die VdS-Richtlinien zum Datenschutz, sondern auch der DS-BVD-GDD-## zur Auftrags(daten)verarbeitung und Prüfsigelansätze wie Trusted Cloud oder EuroPriSe. Dennoch sind die umfassenden Verzeichnisse wertvoll, um sich schnell zu einem konkreten Aspekt der Informationssicherheit zu orientieren.

Abschließend bleibt festzuhalten, dass das Buch mit dem Wort Datenschutz im Titel den Mund etwas zu voll nimmt und der bisherige Name dem Werk besser gestanden hätte. Wer jedoch für die tägliche Nutzung ein Kompendium für die Ausarbeitung, Prüfung und Bewertung Technischer und Organisatorischer Maßnahmen sucht, ist mit „Informationssicherheit und Datenschutz“ bestens beraten.

Rezensionen von

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

RECHTSHANDBUCH INDUSTRIE 4.0 UND INTERNET OF THINGS

Thomas Sassenberg, Tobias Faber (Hrsg.)

Sassenberg, Faber (Hrsg.)
»Rechtshandbuch Industrie 4.0 und Internet of Things«

C. H. Beck / Vahlen

2. Auflage 2020
798 Seiten, Hardcover (Leinen)
189,00 Euro
ISBN: 978-3-406-72917-1

Das Vorwort verweist darauf, dass die Begriffe „Industrie 4.0" und „IoT – Internet of Things" vor allem Schlagworte der industrie- und standortpolitischen Diskussion sind. Nach der Einführung werden unter der gleichlautenden Überschrift des Kapitel 2 „Typische Fragen" beahndelt: Schutz von maschinengenerierten Daten; Forschung und Entwicklung sowie Kooperationen; Haftungsfragen bei vernetzten und autonomen Systemen; Anforderungen des Telekommunikationsrechts; Datenschutz und IT-Sicherheit; Kartellrechtlicher Rahmen; Arbeitsrecht – Realität und Herausforderungen; (neu in der 2. Auflage:) Gesellschaftsrecht. In Kapitel 3 werden die Besonderheiten bei Vertragsschluss und -gestaltung ausgeführt. Gerade das in diesem Kontext nicht leicht anzuwendende Telekommunikationsrecht erhält den erforderliche Raum. Das Unterkapitel „Vertragstypen und Herausforderungen der Vertragsgestaltung" enthält eine – auch für Nichtjuristen – gelungene Aufbereitung von Vertragsinhalten und Gestaltungsrahmens und schließt mit einer Checkliste. Kapitel 4 ist neu in der 2. Auflage und behandelt die Themen „Künstliche Intelligenz und Machine Learning" sowie Block Chain. Unter der Überschrift „Besonderheiten ausgewählter Branchen" werden die Digitalisierung des Gesundheitswesens, Automatisiertes Fahren (Automotive), Digitalisierung des Energiesektors (Smart Grids), Digitalisierung der Versicherungswirtschaft (Insurance), Digitalisierung der Elektroindustrie (Smart Factory), Digitalisierung der Bankenwelt (FinTech) und (neu in der 2. Auflage) „Aviation – Unbemannte Luftfahrzeuge" behandelt. Das Werk schließt mit „Europäische und amerikanische Perspektiven" in Kapitel 6. Die Attraktivität des Werkes leitet sich aus der Zweiteilung aus juristischen Themen und Branchenperspektive ab. Das Werk ermöglicht damit eine grundlegende Befassung und Einarbeitung in die einzelne rechtliche Fragestellungen, aber auch eine direkte branchenrelevante Befassung. Der Leser muss sich aber – und das ist keine Kritik – bewusst sein, dass es sich um ein Rechtshandbuch handelt. Das Werk ist daher nicht als Einführung für Nichtjuristen konzipiert, aber dennoch gut verständlich.

Insgesamt bietet das Werk einen umfassenden, aktuellen Überblick. Auch wenn man bei der Bewertung nicht immer die Meinung der Autoren teilt, ändert dies nichts an der Qualität der Darstellung. Gerade bei neuen, nicht in allen Facetten gerichtlich geklärten Themen liegen unterschiedliche Ansichten in der Natur der Sache. Das Werk kann daher zum Kauf uneingeschränkt empfohlen werden und ist jedem, der sich mit dem Thema rechtlich befasst, zur Lektüre und als Nachschlagewerk angeraten.

Rezension von

Dr. Jens Eckhardt
Rechtsanwalt und Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV), Compliance-Officer (TÜV), dmp Derra Meyer & Partner Rechtsanwälte, Düsseldorf, Ulm, Berlin und Mitglied im Vorstand des BvD e. V.

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:

03.09.2020	RG Ost	**30.10.2020**	RG München
21./22.09.2020	AK Medizin	**05.11.2020**	RG Nord
24.09.2020	RG Gütersloh	**06.11.2020**	AK EVU
02.10.2020	RG Karlsruhe	**13.11.2020**	RG Schwäbisch Gmünd
16.10.2020	RG Stuttgart		
23.10.2020	RG Nürnberg		
30.10.2020	AK Krypto		

Bitte beachten Sie:

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

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

Termine und Anmeldung finden Sie auf unserer Webseite:

▶ www.bvdnet.de

VERNETZEN SIE SICH MIT UNS:

▶ www.bvdnet.de

XING: www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands

TWITTER: www.twitter.com/bvd_datenschutz

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

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

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

BVD-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

Jetzt 3 Monate ZD kostenlos testen und Geschenk sichern!

IHR GESCHENK

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

Die große Zeitschrift zum Datenschutz

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

Geschaffen für die Unternehmenspraxis

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

Alles inklusive:

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

3 Hefte gratis

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

ZD – Zeitschrift für Datenschutz

10. Jahrgang. 2020. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 269,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS
sowie für ausgewählte Kooperationspartner € 209,–

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebsgebühren € 14,40 jährlich.

beck-shop.de/go/ZD

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

C.H.BECK