Ausgabe 01/2019

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Ein Gesetz lernt laufen – wie die DS-GVO in der Praxis angekommen ist

CHANCEN UND RISIKEN DER DS-GVO – ab S. 5

ALS COMPLIANCE SCHOCKTE – EIN RÜCKBLICK AUF 2018 – ab S. 22

INTERVIEW MIT BFDI ULRICH KELBER – „DATENSCHUTZBEAUFTRAGTE BEDEUTEN KEINEN BÜROKRATIEAUFWAND“ – ab S. 58

DIE DATENSCHUTZAUFSICHT – HANDELN MIT SCHARFER KLINGE – ab S. 70

BvD e.V.
DATENSCHUTZ GESTALTEN

30 Jahre BvD

Gemeinsam für einen starken Datenschutz!

30 Jahre Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

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

Der BvD in Zahlen:

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

(Stand: Januar 2019)

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

DIE DS-GVO LERNT LAUFEN

Liebe Leserinnen und Leser,

lange haben wir auf den Startschuss geschaut und so schnell kann die Zeit vergehen: Die DS-GVO lernt laufen und feiert demnächst schon ihren ersten Geburtstag. Jeder von uns hat ein bewegtes Jahr hinter sich – und der Datenschutz eine Phase höchster Aufmerksamkeit in Unternehmen und Institutionen, aber auch in der Medienlandschaft. Für den Datenschutz ist viel Gutes getan worden, einiges war mehr schädlich als hilfreich, aber eines lässt sich nicht von der Hand weisen. Datenschutz hat heute eine andere Bedeutung als noch vor wenigen Jahren. Wichtige Prinzipien der DS-GVO haben Fuß gefasst, im Umgang mit personenbezogenen Daten – wichtiger Wegbegleiter dabei ist der betriebliche oder behördliche Datenschutzbeauftragte. Es hat sich gezeigt, dass der Datenschutzbeauftragte allein durch die Wahrnehmung seiner gesetzlichen Aufgaben zum Gestalter des Datenschutzes in Unternehmen und Institutionen wurde. Dies setzt jedoch voraus, dass er die Gelegenheit zu direkter Kommunikation im Unternehmen und aktiver Teilnahme an Abstimmungen und Planungen wahrnimmt und seine Fachkompetenz einbringt. Die Zeiten für die Versender von „One-size-fits-all-Checklisten" dürften endgültig zu Ende gehen. Dies zeigen auch die Beschwerden von Unternehmen, die solchen „Beratern" zunächst auf den Leim gegangen sind, bald aber feststellen mussten, dass diese nicht wirklich weiterhelfen konnten.

Die Bedeutung von Know-how und Fachkunde zeigt sich umso mehr, wenn wir einen Blick auf das Hauptthema unserer diesjährigen BvD-Verbandstage werfen: „Künstliche Intelligenz und die DS-GVO – (k)ein Konflikt?". Nachdem die Digitalisierung in weite Teile der Unternehmensprozesse Einzug gehalten hat, eröffnen sich durch den Einsatz von Maschinenlernen in Big-Data-Umgebungen durch Künstliche Intelligenz weitere Geschäfts- und Verarbeitungsmodelle, deren Vereinbarkeit mit dem Datenschutz erst noch zu bewerten ist. Mit diesem Themenschwerpunkt auf den Verbandstagen möchten wir zeigen, wie der aktuelle Stand in diesem Bereich ist und dass die DS-GVO durchaus geeignete Instrumente bereit hält, um auch den Einsatz neuer Technologien unter Wahrung der Rechte und Freiheiten der betroffenen Personen zu ermöglichen.

Neben spannenden Vorträgen bieten die Verbandstage die zweite DAME-Preisverleihung, die wiederum mit sehr spannenden Preisträgern und Initiativen aufwarten kann. Ganz nebenbei wird der BvD dieses Jahr auch 30 Jahre alt. Dies zwar erst im Oktober, trotzdem erlauben wir uns auch zu den Verbandstagen schon ein wenig zu feiern. Dabei ist der BvD nicht alt sondern in seinen besten Jahren (die dauern ja bekanntlich länger an) und hat eine Menge an Ideen und Themen zu bieten, wie Sie dem Programm der Verbandstage entnehmen können.

Ich wünsche Ihnen eine interessante Lektüre und hoffe, wir sehen uns im Juni zu den Verbandstagen!

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:

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

Fotos:

123rf.com, shutterstock.com

Lektorat:

Frank Spaeing, Regina Mühlich

Anzeigen:

Katrin Eggert
(bvd-gs@bvdnet.de)

Satz und Layout:

Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

Druck:

Trend Point Marketing GmbH,
Breitenbachstraße 24-29, 13509 Berlin
www.tpmarketing.de

ISSN: 2194-1025

Erscheinungsweise: 3 x jährlich, ca. 3.500 Exemplare (Mediadaten anfordern unter bvd-gs@bvdnet.de)
Die Redaktion behält sich vor, Beiträge redaktionell zu überarbeiten und zu kürzen. Namentlich gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

EDITORIAL

Die DS-GVO lernt laufen – *Thomas Spaeing* 3

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Chancen und Risiken der DS-GVO – *Dr. Lambert Gneisz und Mag. Andreas Schütz, LL.M.* 5

E-EVIDENCE

e-Evidence: Unpraktikabel und rechtlich zweifelhaft – *Peter Schaar* 10

KI & DIGITALISIERUNG

Künstliche Intelligenz und Datenschutzrecht – ein Überblick – *Fritz-Ulli Pieper, LL.M.* 14

Das Auto als totaler Überwacher des Fahrers? – *Marion Jungbluth* 18

DATENSCHUTZPRAXIS

Als Compliance schockte – ein Rückblick auf 2018 – *Dr. Niels Lepperhoff* 22

Die Umsetzung der EU DS-GVO im Unternehmen – Bericht aus der Praxis – *Timo Ahland* 26

„Eine kurze Nachfrage…" – DS-GVO-konforme Identitätsprüfung bei der Erfüllung von Betroffenenrechten – *Dr. Carlo Piltz und Melanie Pradel* 28

Anforderungen an die datenschutzrechtliche Wirksamkeit der Einwilligung – *Prof. Dr. Jürgen Taeger* 32

50-Mio.-Euro-Strafe für Google: Eine kritische Bewertung der Bußgeldentscheidung der französischen Datenschutz-Aufsichtsbehörde CNIL – *Dr. Tilman M. Dralle* 38

Sind private Messenger-Dienste für die unternehmensinterne Kommunikation unter Mitarbeitern geeignet? – *Lena Bäumges* 42

Das berechtigte Interesse als Rechtfertigungsgrund - eine praxisnahe Darstellung – *Jutta Oberlin und Dr. Lukas Lezzi* 45

Unterschätzte Herausforderung: Die Nachweispflichten nach Art. 5 und 24 DS-GVO entwickeln sich zum Knackpunkt der Umsetzung – *Interview mit Christian Volkmer* 54

AUFSICHTSBEHÖRDE

Interview mit BfDI Ulrich Kelber – *„Datenschutzbeauftragte bedeuten keinen Bürokratieaufwand"* 58

Websites im Datenschutzcheck am SID 2019: Was Websitebetreiber wissen sollten, um Datenschutzverstöße zu vermeiden – *Alexander Buckel* 61

Schulstunden der etwas anderen Art oder: Datenschützer und Schüler lehren und lernen gemeinsam – *Am Safer Internet Day (SID)* 66

Die Datenschutzaufsicht - Handeln mit scharfer Klinge – *Maria Christina Rost* 70

GESELLSCHAFT

Neue Verfügungsrechte an Daten - Eigentum als Chance oder Risiko? – *Prof. Dr. Anne Riechert* 74

Facebook und der Datenschutz – ein Fall für das Bundeskartellamt? – *Prof. Niko Härting* 76

Facebooks unsichtbare Datensammlung – *Miriam Ruhenstroth* 78

AUS DEM VERBAND

DAME 2018: „Datenschutz ist in der Gesellschaft angekommen" – *Jury nominiert drei Produktionen für BvD-Medienpreis 2018* 83

BvD Newcomer-Forum – *Jürgen Hartz* 86

Überblick Seminare und Workshops 2019 87

REZENSIONEN

„Datenschutzrecht - DS-GVO mit BDSG" – *Simitis, Hornung, Spieker (Hrsg.)* 88

„Big Data und Recht – Einführung für die Praxis" – *Calderola / Schrey* 89

„Das neue Datenschutzrecht in der betrieblichen Praxis" – *Laue / Kremer* 90

Digitalisierte Verwaltung – Vernetztes E-Government – *Margrit Seckelmann (Hrsg.* 91

Datenschutz im Krankenhaus – mit allen Neuerungen durch die DS-GVO – *Andrea Hauser/Ina Haag* 92

Arbeitsrecht 4.0 - Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt – *Arnold/Günther* 94

Datenschutz nach der EU-Datenschutz-Grundverordnung (BDSG 2018) – *Jochen Schneider* 95

DATENSCHUTZ-GRUNDVERORDNUNG General Data Protection Regulation – *Thomas Müthlein (Hrsg.)* 96

TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 97

CHANCEN UND RISIKEN DER DS-GVO

Dr. Lambert Gneisz und Mag. Andreas Schütz, LL.M.

Mit über 4.000 Änderungsanträgen war die DS-GVO im Europäischen Parlament das am intensivsten diskutierte Gesetz aller Zeiten! Heftige Diskussionen begleiten den Umgang mit der DS-GVO oft bis heute, wenn es darum geht das Gesetz dem Praktiker verständlich zu machen, es sinnvoll anzuwenden und seinen Nutzen für die Wirtschaft zu realisieren.

Was bedeutet die DS-GVO in der betrieblichen Praxis, am Beginn des zweiten Quartals im Jahr 2019? Wie kann die betriebliche Datensicherheit gesetzeskonform angehoben und abgesichert werden, um nicht das Risiko der massiv formulierten Strafen bei Nichteinhaltung einzugehen? Welche wirtschaftlichen Vorteile sind für Unternehmen bei intelligenter Erfüllung der neuen Rechtsvorschriften möglich? Zu diesen Fragen kamen zahlreiche weitere dazu:

- Gilt die DS-GVO auch für Ein-Personen-Unternehmen (EPU) und Vereine?
- Wie kann das erforderliche DS-GVO-Wissen in der Organisation verankert werden?
- Ist die verschärfte Geschäftsführerhaftung der stärkste „Motivator" zur DS-GVO-Compliance?

Dieser Artikel stellt erfolgsbewährte Maßnahmen zur Erfüllung von DS-GVO-Anforderungen dar. Er soll für den Entscheidungsträger eine Hilfe sein, Chancen und Risiken bei der Bewältigung der Datenschutzverpflichtungen zu verstehen und erfolgreich zu bewältigen.

Insbesondere werden die betrieblichen Vorteile beleuchtet, die für Unternehmen bei einer professionellen DS-GVO-Umsetzung etwa zu einer Verbesserung der Wettbewerbssituation erreicht werden können.

1. Gilt die DS-GVO auch für EPU und Vereine?

Trotz der Hoffnung auf Ausnahme oder günstigere Regelungen hinsichtlich kleinerer Unternehmensstrukturen wie EPU und gemeinnütziger Vereine treffen auch diese die Bestimmungen der DS-GVO sowie grundsätzlich auch nationale datenschutzrechtliche Bestimmungen.

Auch wenn sich insbesondere für Vereinskooperationen oder Fund-Raising Spezialfragen (Dürfen gleichartige Vereinigungen über einem Dachverband Interessentendaten austauschen? ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Was geschieht mit Daten nach Vereinsauflösung? etc.) ergeben, ist es für den Datenschutz letztendlich unerheblich, ob Daten aus kommerziellen oder gemeinnützigen Zwecken ermittelt, verwendet oder übermittelt werden.

Da die Ausnahmeregelungen der DS-GVO abschließend sind und EPU und Vereine (unabhängig ihrer Größe) auch nicht miteinbeziehen, haben sich diese somit in gleichem Maß an die DS-GVO zu halten wie Unternehmen.

2. Wie teuer sind IT-Risiken?

Fast alle Geschäftsprozesse erfordern heute die IT-Nutzung. Risiken, die aus dem Einsatz der Informationstechnologie im Unternehmen stammen, verdienen daher besondere Betrachtung und besonderen Schutz. In der betrieblichen Praxis bietet schon alleine dieser Punkt wertvolle Möglichkeiten durch DS-GVO-Compliance das Unternehmensrisiko verbessert abzusichern. Denn das typischerweise spontane Eintreten von IT-Risiken, etwa durch die stark ansteigende Anzahl von Cybercrime-Fällen, kann unerfreulich rasch zu sehr wesentlichen bis hin zu existenziellen Schwierigkeiten führen.

Ein risikoorientiertes Management der Informationstechnologie ist heute mehr denn je unabdingbar und kann nur Hand in Hand mit der Erfüllung der DS-GVO-Pflichten gesehen werden. Stark wachsend in ihrem Risikogehalt sind etwa die Herausforderungen des Outsourcings und der Nutzung von IT-Services aus der Cloud. Ob im Gesundheitswesen, im bargeldlosen Zahlungsverkehr oder bei dem Betrieb von kritischer Infrastruktur.

Daher sind in DS-GVO-Projekten, abgesehen von der Geschäftsführung, der Personalleitung und der Rechtsabteilung zwingend auch der Chief Information Officer (CIO) der IT-Services einzubinden. Zu beachten ist dabei, dass der CIO nicht zum Datenschutzbeauftragten ernannt werden sollte.

3. DS-GVO-Risiken kalkulieren und als Kosten sichtbar machen

Es empfiehlt sich, erwartete Risiken z. B. als Ergebnis einer Datenschutz-Folgenabschätzung (DSFA) in kaufmännischen Größen, etwa in abgezinsten Barwerten zu kalkulieren und dafür in den zukünftigen Bilanzen vorzusehen.

Dieses Vorgehen, das auch der Gesetzgeber durch dessen Auftrag zur unternehmerischen Sorgfalt erwartet, wird empfohlen. Es beeinflusst erfahrungsgemäß das Bewusstsein und die Aufmerksamkeit von Entscheidungsträgern in Organisationen positiv.

4. Vorgehen zur Risikoerfassung und Risikobewertung

Risiken lassen sich nicht ausschließen, daher sind organisatorische Vorbereitungen für das Risikomanagement zu treffen. In Abstimmung auf die Anforderungen der DS-GVO empfiehlt sich ein Vorgehen in fünf Schritten:

- Identifikation von Risiken (Gap Analysis), z.B. in Zusammenarbeit mit externen Beratern
- Technische Bewertung von Risiken (Risk Analysis), u.a. mit Benchmarks
- Unternehmerische Bewertung von direkten Risiken (Business Impact Analysis)
- Bewertung von rechtlichen Haftungsrisiken (Legal Impact Analysis)
- Bewertung von rechtlichen sonstigen Risiken (Public Impact Analysis)

5. Mögliche betriebliche Vorteile aus DS-GVO-Aktivitäten

Positive Effekte von DS-GVO-Projekten sollen unbedingt in die kaufmännische Gesamtbetrachtung integriert werden.

Zu vier übergeordneten Nutzenkategorien:

- Sicherheit
- Kosten
- Wettbewerb
- Compliance

können zwölf mögliche Veränderungsvorteile zu jedem DS-GVO-Projekt erfasst und in ihrer Entwicklung dokumentiert werden:

1. Erhöhte Sicherheit im IT-Betrieb
2. Vermeidung von Kosten durch Produktionsausfälle (unproduktive Zeiten)
3. Qualitätssicherung durch Qualitätsmanagement
4. Kostensenkung durch Prozessoptimierungen
5. Erhöhung von Produktivität und Wertschöpfung
6. Ausbau des Vorsprungs gegenüber dem Mitbewerb
7. Positives Zeichen an Mitarbeitende für mehr Mitarbeitermotivation und Loyalität
8. Erhöhung der Rechtssicherheit im Allgemeinen
9. Anhebung des Compliance-Niveaus
10. Absicherung der Geschäftsführerhaftung
11. Verbesserung des Images am Markt, wie z.B. Employer Branding
12. Erhöhung des Vertrauens von Eigentümern, Kapitalgebern, Aufsichtsrat und nationalen Datenschutzbehörden.

6. Die Gefahr der Wahrnehmungsschwelle

Risiken sind für Unternehmer „das tägliche Brot“. Daher besteht die latente Gefahr, dass neue Risikothemen übersehen oder unterschätzt werden, oder beides. Zwar werden Risiken auch durch die beste vorausschauende Planung nicht zu vermeiden sein. Doch können und müssen ihre Auswirkungen durch vorbereitende Maßnahmen zur Risikosteuerung nachweislich verringert werden. Die professionelle Umsetzung der DS-GVO-Vorgaben, etwa jener aus Artikel 32, ist dafür eine sehr gute Gelegenheit, auch mit hohem risikopolitischem Nutzen.

Sollte ein Schaden eintreten, so wird es bei der Beurteilung von Haftungsfragen wesentlich sein belegen zu können, welche adäquaten Aktivitäten zur Schadensvermeidung vorab getroffen wurden. Darin liegt eine Verantwortung der Geschäftsführung. Insbesondere, da in der Literatur auch die Meinung vertreten wird, dass einzelne Regelungen der DS-GVO als Schutzgesetze anzusehen sind. Das hat zur Folge, dass Pflichtverletzungen im Datenschutzbereich auch den Geschäftsführer haftbar machen könnten, wenn dieser die Grundsätze der „fachlich einwandfreien Leitung eines Unternehmens“ verletzt. Auch kann sich dieser nicht auf mangelndes Wissen oder mangelnde Fähigkeiten berufen, da er die Geschäftsführerfunktion sonst nicht hätte übernehmen dürfen.

Durch die professionelle Planung eines Datenschutzprojektes kann den Gefahren der fahrlässigen beziehungsweise vorsätzlichen Geschäftsführerhaftung begegnet werden. Jede Organisation hat die Möglichkeit, durch Vorbereitungsmaßnahmen in einem vom jeweiligen Unternehmen gewünschten Ausmaß, ein neues Sicherheitsniveau zu schaffen und erfolgreich auszubauen!

7. Projektablauf

Die vielfältigen Anforderungen der DS-GVO können zumeist nicht zeitgleich und vollständig erfüllt werden. Das Unternehmen muss daher abschätzen und priorisieren, welche Verarbeitungen von personenbezogenen Daten das größte Risiko für den Geschäftsbetrieb des ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Unternehmens und / oder die Rechte der betroffenen Personen darstellen sowie welche Risiken am wahrscheinlichsten zu hohen Geldbußen führen können. Im Anschluss an diese Einschätzung sind die Ressourcen entsprechend umfangreich und vor allem zeitnah bereitzustellen. Da die Vorbereitung auf die DS-GVO eine gründliche Analyse, möglicherweise auch eine Restrukturierung sehr vieler interner Prozesse erfordert, ist es höchst empfehlenswert rasch auf die Anforderungen von technischen und organisatorischen Maßnahmen (TOMs) zu reagieren.

8. DS-GVO-Implementierung mit „Gap Analysis“

Zur Feststellung des datenschutzrechtlichen Handlungsbedarfs eines Unternehmens sollten zuerst rechtliche, organisatorische und IT-technische „Lückenanalysen“ durchgeführt werden. Dabei wäre die gegenwärtige Datenschutz-Compliance mit den Anforderungen der DS-GVO abzustimmen. Der nächste Schritt besteht in einer Risikoanalyse, mit bereichsübergreifenden und daher für Entscheidungsträger sehr relevanten kaufmännischen Bewertungen von juristischen, technischen und organisatorischen Risiken in einer Zusammenschau. Unbedingt betrachtet werden müssen in dieser Phase auch die Risiken der persönlichen Haftung und in welchen denkbaren Schadensfällen diese wie schlagend werden könnten.

9. Projektsteuerung und Ressourcen-/ Budgetplanung

Die Kosten eines DS-GVO-Projekts können als Investition („Einzahlung“) in eine „Datenschutzrisiko-Versicherung“ verstanden werden.

Wie die betriebliche Praxis zeigt, waren auch zu Jahresende 2018 nur wenige Organisationen auf die immerhin bereits seit April 2016 bekannten DS-GVO-Anforderungen vollständig vorbereitet. Warum war das so? Die erforderlichen Ressourcen waren oft intern schlichtweg nicht gegeben.

Eine zweckmäßige Lösung, zumindest zur Bearbeitung der „größten DS-GVO-Brocken“ ist die Zusammenarbeit mit dafür qualifizierten externen Partnern, wie Rechtsanwälten, Unternehmensberatern, IT-Consultants. Zwei Gründe sprechen vor allem dagegen zu glauben, sich in dieser Situation, wie der berühmte Baron Münchhausen „am eigenen Schopf aus dem Schlamm ziehen“ zu können:

Die Materie ist schlichtweg zu komplex, um sie in wenigen Tagen zu erlernen.

Die möglichen operativen und strategischen Schäden sowie die umfassenden Haftungsrisiken sind zu massiv, um sie „auf die leichte Schulter“ zu nehmen.

10. Im Überblick: Umsetzung einer Datenschutz-Struktur

Die DS-GVO enthält eine Reihe zusätzlicher wesentlicher Anforderungen im Verhältnis zum bisher geltenden Recht:

1. Stärkere Rechte der betroffenen Personen (z.B. auf Information, Auskunft und Berichtigung/Löschung; das Recht auf Datenübertragbarkeit; das Recht auf Widerspruch gegen bestimmte Datenverarbeitungstätigkeiten; das „Recht auf Vergessenwerden“ – die Verpflichtung der Verantwortlichen, Auskunfts- oder Löschanträge an dritte Datenempfänger weiterzuleiten; strengere Anforderungen an Einwilligungserklärungen etc.).

2. Strengere organisatorische Anforderungen (z.B. die Verpflichtung, ein Verfahrensverzeichnis von internen Datenverarbeitungstätigkeiten zu erstellen und fortan zu führen; die Notwendigkeit, in verschiedenen Fällen eine Datenschutz-Folgenabschätzung durchzuführen ggf. und einen Datenschutzbeauftragten zu benennen; Datenschutz durch Technik („privacy by design“) und Datenschutz durch datenschutzrechtliche Voreinstellungen („privacy by default“); die Verpflichtung zur Verknüpfung personenbezogener Daten mit dem Zweck ihrer Erhebung und der Ermächtigungsgrundlage für ihre Verarbeitung; die Dokumentation von Datenübermittlungen; Erstellung diverser Löschungskonzepte etc.).

3. Strengere Meldepflichten (z.B. die Verpflichtung im Falle einer Verletzung des Schutzes personenbezogener Daten binnen 72 Stunden die Datenschutzbehörde sowie ggf. die betroffenen Personen zu informieren).

4. Höhere Cyber-Sicherheitsanforderungen an die IT

5. Strengere vertragliche Anforderungen (mit externen Service-Providern, Auftragsverarbeitern und unter Umständen auch innerhalb der Unternehmensgruppe).

Um allen Verpflichtungen nachzukommen, von denen massive kaufmännische Risiken ausgehen können, muss das Unternehmen eine robustere Datenschutzstruktur einführen.

11. Datenschutz-Management-System

Die DS-GVO sieht eine Reihe von Anforderungen vor, die ohne ein umfassendes Datenschutz-Management-System schwierig zu bewältigen sind. Ein solches System sollte unternehmensweit eingeführt werden, da datenschutzrechtliche Verstöße selbst kleiner Niederlassungen zu hohen Geldbußen für eine gesamte Unternehmensgruppe führen können.

Viele der Verpflichtungen aus der DS-GVO können in der Praxis nur implementiert werden, wenn entsprechende Konzepte, Richtlinien und Standardvorgehensweisen (kumulativ sog. „Standard Operating Procedures“, „SOP“) zur Qualitätssicherung eingeführt werden. Dies betrifft insbesondere die Rechte betroffener Personen, die Meldepflichten bei der Verletzung des Schutzes personenbezogener Daten und die Datenschutz-Folgenabschätzungen.

Darüber hinaus müssen Mitarbeiter in Bezug auf ihre sich aus der DS-GVO ergebenden Verpflichtungen und Verantwortlichkeiten geschult werden. Das Unternehmen hat angemessene Maßnahmen zu ergreifen, um die Einhaltung der Anforderungen der DS-GVO nachzuweisen. Diese Maßnahmen sollten regelmäßig überprüft und aktualisiert werden.

12. Resümee

Aufgrund der hohen Anzahl von Vereinbarungen, die unternehmensintern sowie mit Dritten geschlossen werden müssen, ist eine durchdachte Strategie für das Management von Datenverarbeitungsverträgen zu definieren und umzusetzen.

Dabei ist eine externe professionelle Begleitung der effektivste Weg, um für die gegebenen großen Risiken das gewünschte Sicherheitsniveau etablieren und halten zu können und weiters, um die genannten mehrdimensionalen Wertschöpfungsvorteile aus professionell umgesetzten DS-GVO-Projekten realisieren zu können.

Über die Autoren

Dr. Lambert Gneisz

ist Unternehmensberater, Gründer und Inhaber der Performer Management Instruments Dr. Gneisz GmbH in Wien sowie Gerichtssachverständiger für Unternehmensberatung, von der TÜV-Akademie zertifizierter Datenschutzbeauftragter nach ISO/IEC 17024; Zertifizierter Data & IT-Security Experte.

Mag. Andreas Schütz, LL.M.

ist CEE Partner der internationalen Anwaltssozietät Taylor Wessing. Er ist, unter anderem, anerkannter Experte in sämtlichen Bereichen des IT-Rechts, insbesondere im Technologiesektor sowie im Datenschutz, Software Lizenzen & Vertriebsrecht, E-Commerce, Werberecht und Unlauterer Wettbewerb.

- www.dsgvo-performer.com
- www.taylorwessing.com

DSGVO PERFORMER® TaylorWessing

E-EVIDENCE

E-EVIDENCE: UNPRAKTIKABEL UND RECHTLICH ZWEIFELHAFT

Peter Schaar

In der Europäischen Union wird mit Hochdruck an zwei Rechtsakten gearbeitet, die Unternehmen dazu verpflichten sollen, Anordnungen von Strafverfolgungsbehörden anderer Mitgliedstaaten zur Sicherung und Herausgabe elektronisch gespeicherter Daten zu verpflichten. Es handelt sich dabei um eine „Verordnung über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen" (e-Evidence-VO) und eine ergänzende Richtlinie für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren. Das E-Evidence-Paket ist das europäische Gegenstück zu dem bereits im Sommer 2018 in Kraft getretenen US-CLOUD Act, der den US-Strafverfolgungsbehörden den Zugriff auf elektronische Daten erlaubt, die außerhalb des US-Territoriums gespeichert sind.

Parallel zu dem Gesetzgebungsprozess in der EU gibt es spätestens seit Mai 2018 Diskussionen auf höchster Ebene zwischen der EU und den USA über den gegenseitigen Datenzugriff von Strafverfolgungsbehörden. Am 05. Februar 2019 hat der Europäische Rat der Kommission das Mandat zur Aufnahme von Verhandlungen mit der US-Regierung zum Zweck einer entsprechenden Kooperationsvereinbarung auf Gegenseitigkeit erteilt. Vor diesem Hintergrund ist eigentlich klar, dass es bei dem e-Evidence-Paket um mehr geht als um die Erleichterung des Zugriffs für Strafverfolgungsbehörden innerhalb des EU-Binnenmarkts.

Der im Frühjahr 2018 von der Europäischen Kommission vorgelegte Entwurf wurde im Dezember 2018 leicht modifiziert vom Rat gebilligt. So fehlt nur noch die Positionierung des Europäischen Parlaments, damit der „Trilog" zwischen den drei maßgeblichen EU-Gremien beginnen kann. Damit ist in diesem Sommer zu rechnen. Der Europäische Datenschutzausschuss hat eine kritische Stellungnahme zu den Entwürfen abgegeben, die jedoch für die übrigen EU-Organe keine bindende Wirkung hat. Auch seitens der europäischen Wirtschaft, insbesondere von den Telekommunikationsunternehmen und von den Internetprovidern, gibt es massive Kritik an dem Vorhaben.

Eine Polizeibehörde oder Staatsanwaltschaft, die bei ihren Ermittlungen - etwa in einer Betrugssache - auf in einem anderen Mitgliedsland gespeicherte Daten zugreifen möchte, muss sich bisher an die Behörden des Staates wenden, wo die Daten verarbeitet werden. Wie mit diesem Ersuchen umgegangen wird, richtet sich nach dem Recht des Staates, auf dessen Territorium die Server stehen. Die Prozeduren hierfür richten sich nach den jeweils anwendbaren internationalen Rechtshilfeabkommen. Die entsprechenden Prüfungen sind vielfach zeitaufwendig und sie führen nicht immer dazu, dass die angeforderten Daten freigegeben werden. Seit kurzem gibt es zudem die Europäische Ermittlungsanordnung (EEA), die das bisherige Verfahren erheblich beschleunigen soll, aber weiterhin die Einschaltung der Behörden des Vollstreckungsstaates vorsieht, der auch für die Durchsetzung ausländischer Ermittlungsanordnungen zuständig bleibt.

Die e-Evidence-Verordnung soll den Strafverfolgungsbehörden nun den Erlass grenzüberschreitender Sicherungs- und Herausgabeanordnungen ermöglichen, die für die betreffenden Unternehmen verbindlich sind, ohne dass dabei eine Behörde des Vollstreckungsstaats oder desjenigen Staats beteiligt ist, dessen Bürger der Betroffene ist. Für die Nichtbefolgung von Anordnungen drohen den Unternehmen hohe Bußgelder.

Gravierende Grundrechtseinschränkung

Die geplanten Rechtsakte sind in mehrfacher Hinsicht bedenklich: Die EU-Verordnung wäre direkt anwendbares Recht in den Mitgliedsstaaten und bedürfte keiner Umsetzung in nationales Recht. Insofern wäre sie der parlamentarischen Mitentscheidung der nationalen Parlamente entzogen, obwohl es sich beim Strafrecht und den strafprozessualen Vorschriften um eine stark durch nationales Verfassungsrecht geprägte Materie handelt - in Deutschland hat vor allem das Bundesverfassungsgericht staatlichen Befugnissen immer wieder strikte Grenzen gesetzt. Aus diesem Grund hat der Europäische Gesetzgeber darauf verzichtet, die Strafverfolgung in den Geltungsbereich der DS-GVO einzubeziehen. Stattdessen gilt für diesen Bereich eine Datenschutzrichtlinie, die es den Mitgliedsstaten ausdrücklich erlaubt, zusätzliche Vorkehrungen zum Schutz personenbezogener Daten festzulegen.

Die Verordnung bewirkt einen erheblichen Einschnitt in die Grund- und Bürgerrechte, denn Sicherungs- und Herausgabeanordnungen müssten von den Anbietern elektronischer Dienste unmittelbar befolgt werden, mit entsprechenden Konsequenzen für die Personen, deren Daten betroffen wären. Dies soll geschehen, obwohl sich die nationalen Rechtsordnungen weiterhin im Hinblick auf die Strafbarkeit, die Höhe von Strafandrohungen und strafprozessuale Sicherungen stark unterscheiden.

Handlungen, die im Anordnungsstaat strafbar sind, nicht aber in dem Staat, in dem die Verarbeitung stattfindet, könnten so Gegenstand einer Herausgabeverpflichtung sein. Anordnungen zur fortgesetzten Speicherung und Herausgabe von Teilnehmer- und Zugangsdaten können sogar für jede Art von Straftaten erlassen werden. Die vorgesehene Vorgabe, Inhalts- und Transaktionsdaten nur bei Straftaten, die im Anordnungsstaat mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren geahndet werden, ist wenig geeignet, die Bedenken zu zerstreuen. Ein Blick in das deutsche Strafgesetzbuch zeigt, dass dieses Kriterium auf eine Vielzahl von Straftaten zutrifft und nicht etwa nur auf Verbrechen oder andere schwere Straftaten.

Dies ist in anderen Mitgliedstaaten nicht anders. So wird Abtreibung in Polen mit einer Freiheitsstrafe von bis zu drei Jahren bestraft. Die Voraussetzung zur Herausgabe wäre damit erfüllt. Ein deutscher Anbieter müsste die Daten an die polnische Strafverfolgungsbehörde herausgeben, die in einem Abtreibungsfall ermittelt. Der Anbieter eines elektronischen Buchhaltungsdienstes oder ein Cloudprovider, bei dem der Arzt einen Account hat, könnten Adressaten entsprechender Herausgabeanordnungen sein. ▸

E-EVIDENCE

Anschaulich wird diese Problematik auch beim Fall des katalanischen Exilpolitikers Puigdemont, gegen den ein spanischer Haftbefehl wegen „Aufruhr" ergangen war. Nach dem Beschluss des OLG Schleswig erfüllte das Tatgeschehen nach deutschem Recht keinen vergleichbaren Straftatbestand. Der von Spanien erlassene Europäische Haftbefehl durfte gegen ihn in Deutschland nicht vollstreckt werden. Gleiches gilt für Belgien, wo sich der Politiker inzwischen aufhält. Nach der e-Evidence-VO wären die deutschen oder belgischen Provider trotzdem zur Herausgabe entsprechender elektronischer Dokumente verpflichtet gewesen, ohne dass die Rechtmäßigkeit durch ein nationales Gericht überprüft würde.

Damit würden Daten an ausländische Stellen übermittelt, bei denen inländischen Behörden eine entsprechende Befugnis nicht zusteht. Auch strafprozessuale Sicherungen im Vollstreckungsstaat – etwa ein nach deutschem Recht vorgesehener Richtervorbehalt – würden umgangen, wenn das Recht des Anordnungsstaats eine gerichtliche Genehmigung nicht vorsieht. Schließlich würden Anforderungen, die etwa das Bundesverfassungsgericht aufgestellt hat, z.B. zum Schutz des Kernbereichs privater Lebensgestaltung, nicht gewährleistet.

Zumutungen für Provider

Völlig unzumutbar würde zudem die Situation auch für die Provider: Ihnen werden Pflichten auferlegt, die sie in einem rechtsstaatlich einwandfreien Verfahren nicht überprüfen können. Nicht nur Gerichte und Staatsanwaltschaften, sondern jede vom Anordnungsstaat bezeichnete zuständige Behörde kann eine entsprechende Anordnung erlassen. Dies können auch Finanz-, Regulierungs- und Verkehrsbehörden oder mit entsprechenden Befugnissen ausgestattete Geheimdienste sein. In den EU-Staaten werden demnach sehr viele Behörden die Befugnis erhalten, grenzüberschreitend die Herausgabe von Daten zu verlangen. Den Unternehmen ist es nicht einmal möglich, seriös zu prüfen, ob eine Behörde die entsprechende Befugnis besitzt, ja sogar, ob es sich überhaupt um eine Behörde handelt. Zwar sollen die jeweiligen Behörden eine Validierung durch Schreiben eines Gerichtes oder einer sonstigen Justizbehörde nachweisen. Dafür soll es jedoch ausreichen, wenn der Absender ein entsprechendes Dokument per Fax übermittelt. Ob das Fax und der darauf enthaltene Stempel einer Justizbehörde echt ist, ist angesichts der sehr kurzen Fristsetzungen (in bestimmten Fällen sind die Unternehmen verpflichtet, die Daten innerhalb von sechs Stunden zu liefern!) kaum zu überprüfen. Entsprechend groß ist die Gefahr, auf eine gefälschte Herausgabeanordnung hereinzufallen und ohne Rechtfertigungsgrund personenbezogene Daten an Dritte zu übermitteln. Bei Nichtbefolgung der Anordnung drohen dem Unternehmen erhebliche finanzielle und strafrechtliche Konsequenzen. Der so bewirkten erheblichen Verletzung der Grundrechte des Betroffenen entspricht zudem ein erhebliches Haftungsrisiko für den Provider, unrechtmäßig Daten herausgegeben zu haben.

Dabei haben die Unternehmen nur in sehr eingeschränktem Umfang die Möglichkeit, die Übermittlung der angeforderten Daten abzulehnen, wenn sie der Ansicht sind, dass ausschließlich aus den in der Anordnung enthaltenen Informationen hervorgeht, dass sie „offenkundig" gegen die Charta der Grundrechte der Europäischen Union verstößt oder offensichtlich missbräuchlich ist.

Massive Kritik aus dem EP und von den Datenschutzbehörden

Das EP hat im September 2018 eine kritische Studie zum Kommissionsentwurf veröffentlicht und am 28. November 2018 hierzu eine öffentliche Anhörung durchgeführt. Zudem hat der Europäische Datenschutzausschuss massive Kritik an den Kommissionvorschägen geübt. In ihrer Stellungnahme vom 26. September 2018 kritisieren die Datenschutzbeauftragten der EU-Mitgliedstaaten, dass die Kommission es versäumt habe, die Notwendigkeit des neuen Instruments überzeugend zu begründen, zumal es verschiedene alternative Instrumente gäbe, die weniger tief in die Grundrechte eingriffen, insbesondere die Europäische Beweisanordnung oder verbesserte Rechtshilfeabkommen. Auch die Frage unterschiedlicher strafrechtlicher und strafprozessualer Bestimmungen in den Mitgliedstaaten werde nicht hinreichend berücksichtigt. Schließlich sei der vorgesehene Zugriff ausländischer Behörden auf von Serviceanbietern gespeicherten Daten nicht rechtssicher zu realisieren, da die Unternehmen keine effektive Möglichkeit hätten, die Rechtmäßigkeit der Anordnungen zu beurteilen.

Angesichts der gravierenden Auswirkungen wäre es zu begrüßen, dass sich die Zivilgesellschaft stärker mit dieser Materie auseinandersetzt, ihre Bedenken offensiv vertritt und gegenüber den nationalen Regierungen und den europäischen Gremien vorbringt.

Die Entscheidungsträger in Brüssel und den europäischen Hauptstädten sehe ich in der Pflicht, die rechtlichen und praktischen Bedenken ernst zu nehmen und zu berücksichtigen. Starke Zweifel sind angebracht, ob das Gesetzgebungspaket in seiner jetzigen Form auf dem Prüfstand der Verfassungsgerichte der Mitgliedstaaten und des Europäischen Gerichtshofs bestehen würden.

Über den Autor

Peter Schaar

Vorstand Europäische Akademie für Informationsfreiheit und Datenschutz e.V. (EAID)

▶ www.eaid-berlin.de

Anzeige

DATENSCHUTZ | SAP SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

Datenschutz-Manager

Das Datenschutzmanagementsystem für den DSB – EU ready

EU ready

> Sofort einsetzbares System um den Überblick im Datenschutz zu behalten und Risiken effektiv zu erkennen und zu behandeln
> Inhaltlich ausgearbeitete Struktur, ausgerichtet an gesetzlichen Vorgaben und internationalen Normen
> Verzeichnis von Verarbeitungstätigkeiten mit mehr als 220 beispielhaften Verarbeitungen inkl. dokumentiertem Schutzbedarf und anpassbaren Templates
> Logbuch zum einfachen und übersichtlichen Verwalten sowie nachhaltigem Dokumentieren der DS-Aufgaben, wie Anfragen, Prüfungen, Schulungen, Datenpannen, offenen Punkten, Terminen und Generieren von Tätigkeitsberichten
> Web-basierte Kollaborationsplattform zur Integration in Ihre Systemumgebung, optimiert für Microsoft SharePoint

JETZT AUCH IN ENGLISCH

BvD e.V. | EuroPriSe Expert

ditis Systeme – Niederlassung der JMV GmbH & Co. KG Heidenheim • ein Unternehmen des Voith Konzerns
Lise-Meitner-Straße 15 • 89081 Ulm • Tel +49 731 509704 - 40 • E-Mail info@ditis.de • www.ditis.de

KI & DIGITALISIERUNG

KÜNSTLICHE INTELLIGENZ UND DATENSCHUTZRECHT – EIN ÜBERBLICK

Fritz-Ulli Pieper, LL.M.

I. Einleitung

Der Einsatz von „Künstlicher Intelligenz" („KI") ist Alltag geworden, sei es beispielsweise im Vertrieb oder im Kundenservice, aber auch im Personalwesen oder in der Wissenschaft. Autonome Prozesssteuerung oder selbstlernende Entscheidungssysteme bieten erhebliche Wettbewerbsvorteile. KI-Programmen liegen komplexe Algorithmen und selbstlernende Systeme zugrunde. Unterstützt wird dies durch die Verfügbarkeit fortschrittlicher Computer und schneller und großer Massenspeicher – und einer großen Menge an Daten („Big Data"). Diese Entwicklung wirft eine Vielzahl rechtlicher Fragen auf. Das Thema KI wurde dementsprechend auch in der juristischen Literatur bereits vermehrt behandelt. Erst zuletzt sind auch Fragen im Zusammenhang mit dem Datenschutzrecht immer mehr in das Licht der Öffentlichkeit gerückt. Dies verwundert, bedenkt man, dass der Einsatz von KI regelmäßig mit dem Einsatz von großen Datenbeständen (Big Data) einhergeht und ferner beispielsweise oft Kunden- oder Bewerberdaten durch KI-Systeme verwendet werden. In diesem Zusammenhang liegt es auf der Hand, dass auch personenbezogene Daten verarbeitet werden. Doch welche datenschutzrechtlichen Besonderheiten ergeben sich beim Einsatz von KI?

II. Was ist KI?

KI ist ein Teilgebiet der Informatik. In der Literatur zu KI ist man sich einig, dass es keine einheitliche Definition des Terminus „Künstlicher Intelligenz" gibt.[1] Im "*Proposal For The Dartmouth Summer Research Project On Artificial Intelligence*" wurde das Problem der KI darin gesehen, eine Maschine dazu zu bringen, als würde sie sich so verhalten, dass sie als intelligent bezeichnet würde, wenn sich ein Mensch so verhalten würde.[2] Die Behauptung, dass Maschinen agieren könnten, als ob sie intelligent wären, nennt man die schwache KI-Hypothese und die Behauptung, dass Maschinen, die das tun, wirklich denken (und nicht einfach Denken simulieren) die starke KI-Hypothese.[3]

Eine (starke) KI kann gegebenenfalls ihr Verhalten verändern, möglicherweise auch über die ursprünglich von Auftraggebern, Entwicklern und Nutzern intendierte Funktionalität hinaus. Hierbei unterstützt das „Maschinelle Lernen". Im Gegensatz zur klassischen Programmierung wird beim maschinellen Lernen der Algorithmus, also die Rechenanleitung, nicht vollständig durch den Programmierer vorgegeben. Stattdessen lernt der Algorithmus anhand von Trainingsdaten (bestenfalls mittels „Big Data"-Technologien), eine bestimmte kognitive Aufgabe zu lösen.[4]
Das maschinelle Lernen umfasst eine Vielzahl von Ansätzen, unter denen die sogenannten künstlichen neuronalen Netzwerke „artificial neural networks (ANNs)" eine bedeutende Rolle einnehmen. Ziel ist es, ein System zu entwickeln, welches durch Training in verschiedenen („tiefen") Schichten eine bestimmte Aufgabe lösen kann.[5] Hierbei wird angemerkt, dass es aufgrund der komplexen Berechnungen unmöglich sei, die hiermit im Zusammenhang stehenden Logiken im Detail nachzuvollziehen, weswegen man von einer „Black Box" sprechen könne.[6]

III. Anwendungsbeispiele

Intelligente, teils lernende Systeme haben ihre wissenschaftliche Nische längst verlassen und sind zuletzt zunehmend in den Fokus der Öffentlichkeit gerückt.[7] 1996 verlor der damalige Schachweltmeister Garri Kasparow die erste Partie seines Sechs-Partien-Wettkampfs gegen den IBM-Computer „Deep Blue" - bis heute ein Meilenstein in der Geschichte der Computerentwicklung und eine Sensation, denn noch nie hatte ein Schachcomputer den amtierenden Schachweltmeister in einer Partie unter Turnierbedingungen besiegt.[8] Erneute Sensation dieser Entwicklung war der Sieg des Google-Computers „AlphaGo" Mitte März 2016 gegen den südkoreanischen Spitzenspieler Lee Sedol im Brettspiel „Go". Die Besonderheit: Das Spiel galt bis dahin als so komplex, dass es weder für Menschen noch für Computer möglich sei, alle Kombinationen durchzurechnen. Kreativität und Intuition verhelfen zu einem guten Spiel. Dennoch, der Computer gewann vier von fünf Spielen, was als großer Fortschritt in der Entwicklung selbst lernender Maschinen und künstlicher Intelligenz gilt.[9] Im September schaffte es schließlich Nvidia, ein selbstfahrendes Auto zu testen, das mit einem autarken und selbstlernenden Algorithmus ausgestattet war. Die Besonderheit: Das Auto folgte nicht einer einzelnen Anweisung, die von einem Ingenieur oder Programmierer zur Verfügung gestellt wurde. Stattdessen stützte es sich ganz auf einen Algorithmus, der sich das Autofahren selbst gelehrt hatte, indem er einen Menschen dabei beobachtete. [10]

Vermehrt treten auch Anwendungsfälle mit konkretem Datenschutzbezug auf. Bewerbungsverfahren werden immer häufiger durch den Einsatz von KI-Software unterstützt. Dies kann Zusammenhänge und Auswahlmechanismen zu Tage fördern, die ganz neue Erkenntnisgewinne ermöglichen. Es entstehen aber auch neue Risiken, die datenschutzrechtliche Relevanz haben. Ende 2018 kam beispielsweise heraus, dass eine KI-basierte Bewerbungssoftware von Amazon systematisch Frauen diskriminierte.[11] Im Kundenkontakt werden ferner Chatbots eingesetzt, die mit dem Kunden interagieren und dessen Service-Anliegen behandeln. Hierbei merkt der Kunde nicht einmal unbedingt, dass er mit einem Bot interagiert. Gleichwohl werden durch den Bot personenbezogene Daten des Kunden verarbeitet. Zudem sind die Abläufe des Bots je nach Situationszusammenhang gegebenenfalls nicht abschließend determinierbar. Auch hier besteht also ein potentielles Risiko für die personenbezogenen Daten der Kunden. Hier treffen Autonomie und Intelligenz von Systemen mit so genannten „Deep Learning"-Ansätzen zusammen. Dies verändert die Art, wie Computer agieren und ihre Entscheidungen treffen.

IV. Datenschutzrechtliche Auswirkungen

Weder in der deutschen noch der europäischen Datenschutzgesetzgebung finden sich Vorschriften, die direkt auf KI Bezug nehmen oder spezifisch KI-Anwendungsfälle regeln. Im Gegenteil statuiert die DS-GVO sogar in Erwägungsgrund 15 einen Grundsatz der Technologieneutralität. Das Thema wird derzeit eher (noch) in politischen Positionspapieren[12] und Expertenkommissionen[13] behandelt. Es fällt bei näherer Prüfung gleichwohl auf, dass die DS-GVO schon jetzt eine Vielzahl an Vorschriften beinhaltet, die beim Einsatz von KI unter Verwendung von personenbezogenen Daten unter Berücksichtigung der technischen Besonderheiten einschlägig sein könnten. Im Folgenden sollen einige Vorschriften erläutert werden, deren Anwendung im Zusammenhang mit dem Einsatz von KI Besonderheiten ausgesetzt ist. ▶

[1] Vgl. beispielhaft Nilsson, Die Suche nach Künstlicher Intelligenz: Eine Geschichte von Ideen und Erfolgen, 1. Auflage 2014, Vorwort; instruktiv insoweit auch Luger, Künstliche Intelligenz. Strategien zur Lösung komplexer Probleme., 4. Auflage 2001, S. 23.

[2] Abrufbar unter http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html. Dieser sowie alle weiteren Hyperlinks zuletzt abgerufen am 25. Februar 2019.

[3] Russel/Norvig, Künstliche Intelligenz - Ein moderner Ansatz, 3. Auflage 2012, S. 1176; ferner wird teilweise noch "Künstliche Superintelligenz" ("Artificial Superintelligence" (ASI)), erwähnt, nach dem Oxford-Philosophen und KI-Vordenker Nick Bostrom "an intellect that is much smarter than the best human brains in practically every field, including scientific creativity, general wisdom and social skills.", vgl. https://nickbostrom.com/superintelligence.html.

[4] Schücker, Telemedicus v. 16.01.2019, http://tlmd.in/a/3382.

[5] Daher auch der Begriff „Deep Learning", Schücker, Telemedicus v. 16.01.2019, http://tlmd.in/a/3382.

[6] Instruktiv Gausling, DSRITB 2018, S. 519, 524; vgl. auch Herberger, NJW 2018, 2825, 2828.

[7] Pieper, InTeR 2018, 1, 4.

[8] Ausführlich zum Hintergrund Johannes Fischer, „Als Deep Blue das Genie Garri Kasparow schlug", Zeit Online vom 11. März 2016, abrufbar unter http://blog.zeit.de/schach/als-deep-blue-das-genie-garry-kasparow-schlug/.

[9] Jo Bager, „Mensch gegen Maschine 1:4 – AlphaGo gewinnt auch das letzte Spiel", Heise Online vom 15. März 2016, abrufbar unter http://www.heise.de/newsticker/meldung/Mensch-gegen-Maschine-1-4-AlphaGo-gewinnt-auch-das-letzte-Spiel-3135188.html.

[10] Will Knight, "The Dark Secret at the Heart of AI", Technology Review vom 11. April 2017, abrufbar unter https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/?set=604130

[11] Rixecker, „Diskriminierung: Deshalb platzte Amazons Traum vom KI-gestützten Recruiting", t3n vom 11. Oktober 2018, abrufbar unter https://t3n.de/news/diskriminierung-deshalb-platzte-amazons-traum-vom-ki-gestuetzten-recruiting-1117076/.

[12] Vgl. die „Strategie Künstliche Intelligenz der Bundesregierung".

[13] Die EU-Kommission hat eine „High-Level Expert Group on Artificial Intelligence" eingesetzt, die Bundesregierung eine „Datenethikkommission".

KI & DIGITALISIERUNG

Beispiel Grundsätze der Datenverarbeitung:

Bei der Verarbeitung personenbezogener Daten müssen die Grundsätze der Datenverarbeitung berücksichtigt werden. Dies ist unter der DS-GVO umso relevanter, als ein Verstoß schon gegen die Grundsätze einen Bußgeldtatbestand darstellt (Art. 83 Abs. 5 lit. a) DS-GVO). Beispielsweise müssen Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden (Art. 5 Abs. 1 lit. b) DS-GVO). Die Zwecke müssen vorab feststehen. Zudem muss die Datenverarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Art. 5 Abs. 1 lit. c) DS-GVO). Dies kollidiert allerdings mit dem Grundgedanken von „selbstlernenden Entscheidungssystemen" und dem „Erkenntnisgewinn"-Potential bei künstlichen neuronalen Netzen. Diese sind eher darauf angelegt, gerade neue Anwendungsfälle auszunutzen und unvorhergesehene Erkenntnisgewinne zu generieren.

Beispiel Rechtsgrundlagen:

Eine Einwilligung gemäß Art. 6 Abs. 1 S. 1 lit. a) DS-GVO muss insbesondere bestimmt und informiert sein. Der Betroffene muss sich ein zutreffendes Bild der beabsichtigten Datenverarbeitung machen können, wobei es auf das Verständnis des Adressatenkreises des Einwilligungsersuchens ankommt.[14] Beispielsweise bei Kunden, Verbrauchern oder Arbeitnehmern als regelmäßig technischen Laien dürfte es daher mit einigem Aufwand verbunden sein, ihnen die Abläufe sowie die Risiken und Chancen der Verarbeitung mittels einer KI-Software bestimmt und informiert zu erläutern. Auch bei der gemäß Art. 6 Abs. 1 S. 1 lit. f) DS-GVO durchzuführenden Interessenabwägung „im engeren Sinne" kann es eine Rolle spielen, ob personenbezogene Daten im Zusammenhang mit KI verarbeitet werden. Ein Gewichtungsfaktor in der Abwägung ist speziell die Art und Weise, in der Informationen verarbeitet werden, sowie der Schweregrad potentieller Gefahrenquellen für den Betroffenen.[15] Für die Interessenabwägung bedeutet das, dass die Verarbeitung im Zusammenhang mit KI-Systemen quasi immer eine Besonderheit darstellt, da hier zum Beispiel beim Einsatz von Machine Learning potentiell undurchsichtige Mechanismen zum Einsatz kommen und unvorhergesehene Ergebnisse erreicht werden („Black Box").

Beispiel automatisierte Einzelentscheidung im Einzelfall einschließlich Profiling:

Häufig wird der Einsatz von KI auch zur Herbeiführung einer automatisierten Entscheidung im Einzelfall gemäß Art. 22 DS-GVO dienen. Erwägungsgrund 71 nennt beispielhaft die Ablehnung eines „Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen". In der Tat dürfte KI insbesondere geeignet sein, auf Basis flexibler Datenbestände und eigener Deep Learning-Erfahrungen, bestimmte Entscheidungen autark herbeizuführen und gegebenenfalls in der Folge auch umzusetzen. Der Verantwortliche muss gemäß Art. 22 Abs. 3 DS-GVO sowie Erwägungsgrund 71 „angemessene Maßnahmen" zum Betroffenenschutz ergreifen. Insbesondere muss der Betroffene „spezifisch unterrichtet" und eine Entscheidung „erläutert" werden können. KI-Entscheidungen sind aber im Regelfall wenig bis gar nicht nachvollziehbar.[16] Weiterer wesentlicher Fallstrick im Zusammenhang mit dem Einsatz von KI zur Generierung von automatischen Entscheidungen sind die Betroffenenrechte. Den Verantwortlichen treffen Informationspflichten und die betroffene Person hat Auskunftsrechte über „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung". Insbesondere bei den Informationen zur involvierten Logik gibt es unterschiedliche Ansichten, wie weit dies zu verstehen ist. Dies geht von der Mitteilung des „Prinzips hinter der Entscheidung" bis hin zur „Offenlegung des Algorithmus"[17] – ein Paradebeispiel für ein Einfallstor der Besonderheiten von KI im Zusammenspiel mit den datenschutzrechtlichen Anforderungen, und in der Praxis nicht zu unterschätzen, stehen doch gegebenenfalls sogar Geschäftsgeheimnisse auf dem Spiel.

Beispiel Datenschutz-Folgenabschätzung:

Ebenfalls stellt sich die Frage, ob bei der Verarbeitung personenbezogener Daten unter Einsatz von KI-Systemen immer eine Datenschutz-Folgenabschätzung erforderlich ist. Art. 35 Abs. 1 DS-GVO bestimmt, dass eine solche „insbesondere bei Verwendung neuer Technologien" erforderlich ist, da hierbei regelmäßig ein hohes Risiko für die Betroffenen vorliegt. Ein solch hohes Risiko bezüglich der Umstände der Verarbeitung könnte aufgrund ihrer Indeterminiertheit immer dann angenommen werden, wenn Deep Learning-Ansätze verfolgt werden. Kurz gesagt: „neuer als KI geht nicht". Der Katalog mit Tätigkeiten gemäß Art. 35 Abs. 4 DS-GVO der Datenschutzkonferenz nennt denn auch den „Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten zur Steuerung der Interaktion mit den Betroffenen oder zur Bewertung persönlicher Aspekte der betroffenen Person".[18] Auch hier zeigt sich, dass beim Einsatz von KI zumindest immer kurz an eine Datenschutz-Folgenabschätzung gedacht werden muss.

V. Ausblick

Die obigen Ausführungen lassen sich – je nach Anwendungsfall – beliebig weiter vertiefen und bei genauem Hinsehen auch auf weitere Anforderungen insbesondere der DS-GVO ausweiten. Beispielsweise im Hinblick auf die Erfüllung der Anforderungen der Betroffenenrechte, da hier Informationen und Mitteilungen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln" sind – bei KI eine echte Herausforderung – oder die Bestellung eines Datenschutzbeauftragten, wenn durch den Einsatz einer KI eine „umfangreiche regelmäßige und systematische Überwachung" durchgeführt wird, ferner in Bezug auf „Privacy by design", insbesondere bei KI-Softwareentwicklung (Was ist hier Stand der Technik? Was könnten bei KI geeignete „Technische und Organisatorische Maßnahmen" sein?) oder schließlich auch im Zusammenhang mit Privilegien für die Forschung, da KI insbesondere auch im Kontext der Forschung eine große Rolle spielt. Ob und wie hier die Anwendung der DS-GVO angemessen umgesetzt werden kann, wird sich sehr bald zeigen. Verantwortliche sollten sich bewusst sein, dass die (begrüßenswerte) Entscheidung zum Einsatz von KI-Systemen gleichwohl potentiell immer auch datenschutzrechtlich beleuchtet werden muss.

Über den Autor

Fritz-Ulli Pieper, LL.M.
Jahrgang 1983, ist Rechtsanwalt und Fachanwalt für Informationstechnologierecht im Bereich Technologie, Medien und Telekommunikation bei Taylor Wessing in Düsseldorf. Er berät nationale und internationale Mandanten in allen operativen Belangen zum IT-, Telekommunikations- und Datenschutzrecht. Sein besonderes Interesse gilt dabei zukunftsträchtigen Fragen des IT- und Internetrechts, insbesondere zum Internet of Things, Künstlicher Intelligenz sowie Big Data."

▶ www.taylorwessing.com

TaylorWessing

[14] Klement in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 7 DS-GVO, Rn. 73.

[15] Schulz in: Gola, Datenschutz-Grundverordnung, Art. 6, Rn. 59; Art. 29-Gruppe, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP217, S. 47.

[16] Daher wird sogar bereits über eine gesetzliche Pflicht zu Schaffung von Nachvollziehbarkeit künstlich intelligenter Entscheidungen diskutiert, siehe Otto, Telemedicus v. 20.02.2019, http://tlmd.in/a/3395.

[17] Vgl. instruktiv Hoeren/Niefhoff, RW 2018, 47, 53.

[18] Datenschutzkonferenz, Liste der Verarbeitungstätigkeiten, für die eine Datenschutzfolgeabschätzung durchzuführen ist, Nr. 11, abrufbar unter https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/DSK_DSFA_Muss-Liste_Version_1_1_Deutsch.pdf.

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

KI & DIGITALISIERUNG

DAS AUTO ALS TOTALER ÜBERWACHER DES FAHRERS?

Marion Jungbluth

‚Unabhängigkeit' und ‚Freiheit' sind Attribute, die viele Deutsche dem eigenen Auto zuschreiben. Das vernetzte und automatisierte Auto wird spätestens in der Mitte dieses Jahrhunderts fahrerlos Menschen und Güter transportieren. Die Hoffnungen, die mit der Automatisierung und Vernetzung der Fahrzeuge verbunden sind, sind groß. Fährt das Auto alleine, beachtet es alle Verkehrsregeln, bremst schneller und zuverlässiger als ein Mensch und spart im besten Fall durch vorausschauendes Fahren Sprit. Es bleibt dem Fahrer überlassen, welchen Tätigkeiten er sich während der Fahrt widmet. Für Autoindustrie und Politik sind die Themen Automatisierung und Vernetzung endlich Lösungen für alte Probleme wie Verkehrsunfälle, Staus und Schadstoffemissionen, die modern, zukunftsfähig und positiv konnotiert sind. Aber auch Autofahrer schätzen nach der Continental-Mobilitätsstudie 2018 schon heute die Vorteile der digitalen Vernetzung, besonders Navigation, Empfehlungen entlang der Strecke und Parkanzeigen.

Der Fortschritt am Auto hat seinen Preis. Damit die Systeme sicher fahren können, werden massiv Daten verarbeitet. Durch (selbstlernende) Programme, in Verbindung mit Kameras und Sensoren, sind die Fahrzeuge in der Lage Umfeld, Hindernisse und Verkehrszeichen selbstständig zu erkennen. Diese Technik ermöglicht es, dass Autos bereits heute auf Autobahnen selbstständig die Spur halten oder überholen können.

Je autonomer ein Fahrzeug unterwegs ist, desto zuverlässiger müssen die Informationen über das Umfeld des Fahrzeugs sein. Kameras nehmen Bilder von anderen Verkehrsteilnehmern, aber auch unbeteiligten Passanten auf, um deren Verhalten vorherzusehen und um Kollisionen zu vermeiden. Je hochauflösender die Bilder sind, desto kritischer wird die Frage des Datenschutzes. Denn erstens können die aufgezeichneten Passanten nicht erkennen, dass sie aufgenommen werden, und zweitens wird es praktisch unmöglich sein, von diesen eine Einwilligung zu erhalten. In Verbindung mit Gesichtserkennung können diese Daten jedoch hochsensibel sein.

Die Vernetzung des Autos mit der Infrastruktur oder mit anderen Fahrzeugen macht den Informationsaustausch in Echtzeit möglich. Neben Informationen über die Straßenlage, über freie Parkplätze und Benzinpreisvergleiche können im Auto Musik und Videos gestreamt sowie soziale Netzwerke besucht werden. In Zukunft werden diese Informationen und Services durch die Vernetzung schneller, zuverlässiger und präziser sein. Die dabei anfallenden Datenmengen lassen allerlei Rückschlüsse auf den Fahrer zu. Schon jetzt sammeln manche Autohersteller Fahrzeug- und Mobilitätsdaten in einem bisher nicht gekannten Umfang. Dabei werden die Daten nicht nur in der Werkstatt aus einem Speicher ausgelesen, sondern auch über Fernzugriff. Services weisen nicht nur auf die nächste Inspektion hin, sondern warnen proaktiv bei Problemen am Fahrzeug oder über Systemfehler. Das Datensammeln ist besonders kritisch, wenn Standortdaten enthalten sind. Denn daraus lässt sich leicht ein Bewegungsprofil erstellen, das viele Hinweise auf die Lebensweise des Fahrers gibt. Neben Informationen über Freizeit- und Konsuminteressen, Berufstätigkeit und Arztbesuche sind auch Rückschlüsse auf die Fahrweise und Gesetzestreue (Geschwindigkeitsübertretungen etc.) möglich.

Solange das Fahrzeug nicht ohne Fahrer auskommt und die Fahraufgabe vom Menschen und der Maschine ausgeübt wird, besteht die Herausforderung in der Übergabe und in der Sicherstellung der notwendigen Konstitution des Fahrers. Dazu werden der Zustand und das Verhalten des Fahrers überwacht und diese Daten gespeichert. Auf europäischer Ebene wird gerade entschieden, ob eine Reihe zusätzlicher Systeme – wie z. B. Fahrer-Müdigkeitserkennung und -Aufmerksamkeitsüberwachung – verpflichtend in Neufahrzeuge eingebaut werden müssen (General Safety Regulation, Draft 17.05.2018), um die allgemeine Sicherheit zu erhöhen. Damit sich die Fahrerin oder der Fahrer im Falle eines Unfalls entlasten können, muss gespeichert werden, wann das System die Fahrzeugführung innehatte. Mit dem Ziel der allgemeinen Sicherheit wird die Datenverarbeitung im Auto massiv vorangetrieben. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, fordert daher zu Recht, dass das virtuelle Leben von Autofahrern besser geschützt werden muss (Tagesspiegel Background, veröffentlicht am 01.01.2019).

Die Datenschutz-Grundverordnung (DS-GVO) bildet dabei den regulatorischen Rahmen für personenbezogene Daten. Grundsätzlich sollte ein automatisiertes und vernetztes Auto dabei mit möglichst wenigen personenbezogenen Daten auskommen (Datensparsamkeit). Alle Daten, die mit der Fahrzeugidentifikationsnummer (FIN) oder dem Kfz-Kennzeichen oder einer anderen elektronischen Identifikation verknüpfbar sind, gelten bei der Nutzung von Fahrzeugen als personenbezogen und damit datenschutzrechtlich relevant. Darauf hat sich in einer gemeinsamen Erklärung die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA) am 26.01.2016 verständigt. Mobilitätsdaten ohne Personenbezug liegen nur dann vor, wenn eine funktionierende Anonymisierung die Verknüpfung zu einer Person dauerhaft auflöst.

Mit der DS-GVO sind die Anforderungen für die Verarbeitung von Daten in Fahrzeugen, die durch das Fahrverhalten oder die Fahrzeugnutzung beeinflusst werden und deshalb Rückschlüsse auf die persönlichen Lebensverhältnisse der Verbraucher erlauben, festgelegt. Die Autohersteller müssen sich daran messen lassen, wie sie diese Anforderungen verbraucherfreundlich umsetzen. Die informierte Einwilligung darf nicht mehr in seitenlangen Datenschutzbestimmungen verpackt werden, sondern muss durch technische Lösungen umgesetzt werden. Die beiden Grundsätze „Privacy by Design" und „Privacy by Default" sind dabei zu berücksichtigen. Einige Automobilhersteller haben schon die Chancen eines verbrauchergerechten Datenschutzes erkannt und ermöglichen die Kontrolle der Fahrzeugdaten zum Beispiel über Online-Portale, Apps oder im fahrzeugeigenen Display. Damit Halter und jeder Fahrer ohne Aufwand sein informationelles Selbstbestimmungsrecht beim Autofahren ausüben kann, müssen mit wenigen Klicks im Auto Dienste und deren Datenverarbeitung einfach ab- oder zugeschaltet werden können.

Das Interesse an Mobilitätsdaten ist groß, denn mit jeder Information lässt sich Geld verdienen. Personenbezogene Daten dürfen ausschließlich auf Basis einer informierten Einwilligung und ohne ökonomischen Zwang verarbeitet werden. Aber selbst wenn Autohalter im Prinzip selbst entscheiden können, welche Dienste und Funktionen sie nutzen wollen, ist die Versuchung groß, Daten preiszugeben, wenn dafür Komfortvorteile, Sicherheitsgewinne oder attraktive Rabatte winken.

Telematik-Tarife der Versicherungen basieren auf Fahrdaten, mit deren Hilfe fahrverhaltensabhängige Rabatte berechnet werden. Zwei Tarife werden derzeit angeboten, sogenannte „Pay as you drive"- (PAYD-) und „Pay how you drive"-(PHYD-) Modelle. Während bei „Pay as you drive" nur die gefahrenen Kilometer herangezogen werden, basiert „Pay how you drive" auf Parametern des persönlichen Fahrstils. Dabei werden Daten wie beispielsweise Geschwindigkeiten, hartes Bremsen, schnelles Beschleunigen, Uhrzeiten (beispielsweise wie viele Nachtfahrten), Positionen, Abstand zum vorausfahrenden Fahrzeug, Straßenart (z. B. Landstraße oder Autobahn), Leerlaufzeiten oder das Wetter (z. B. Regen und Schnee) aufgezeichnet, an den Versicherer oder einen externen Dienstleister übermittelt und ausgewertet. Auf der Basis dieser Daten wird dann ein Score berechnet, der die zu erhaltene Prämie oder den Bonus bestimmt. Damit Verbraucher selbstbestimmt entscheiden können, ob ein Telematik-Tarif ihnen ausreichende finanzielle Vorteile bringt, benötigen sie zumindest umfangreiche Informationen über den Algorithmus, der den Score im Detail berechnet.

Telematik-Tarife sind mit gravierenden langfristigen Risiken verbunden. Denn die gespeicherten Daten geben nicht nur Auskunft über die Fahreigenschaft und -tauglichkeit des ▸

KI & DIGITALISIERUNG

Fahrers, sondern verraten auch einiges über seine Persönlichkeit. Autofahrer, die beispielsweise aus beruflichen Gründen häufig nachts fahren und keinen Einfluss auf ihre Arbeitszeit haben, wie zum Beispiel Hebammen, könnten benachteiligt werden. Oder ein bestimmtes Fahrverhalten könnte als riskant eingestuft werden, ohne dass dies dem Autofahrer bewusst ist. Langfristig könnten Fahrer wegen ihres risikoreichen Fahrstils den Versicherungsschutz verlieren oder zu sehr hohen Versicherungsbeiträgen herangezogen werden.

Wenn Telematik-Tarife mit Trackingdaten verknüpft werden, entstehen Persönlichkeitsprofile, obwohl das Erstellen totaler Persönlichkeitsbilder durch das Bundesverfassungsgericht verboten worden ist. Eine besondere Gefahr besteht darin, wenn Versicherungen Bereiche von so genannten Smart-Insurance-Lösungen miteinander koppeln sollten. Also die Fahrdaten mit Vitalitätsdaten, die im Tausch für Nachlässe bei der Berufs- und Risikolebensversicherung generiert werden oder mit Daten aus dem Smart Home.

Für den Einzelnen ist es schwer, die langfristigen Folgen von smarten Versicherungstarifen abzuschätzen. Das spiegelt sich auch in der Ambivalenz von Befragungsergebnissen wieder. Auf der einen Seite halten es in einer repräsentativen Befragung im Auftrag des Gesamtverbands der Deutschen Versicherungswirtschaft (GdV) zwei von drei Deutschen (68 Prozent) für richtig, wenn vorsichtige Autofahrer belohnt oder Raser mehr bezahlen müssen und finden es gerecht, wenn individuelle Daten wie das Fahrverhalten oder Fitness-Werte Einfluss auf Versicherungsprämien haben (Pressemitteilung GdV 28.10.2016). Auf der anderen Seite lehnen in einer kürzlich vom SINUS-Institut zusammen mit YouGov erhobenen Studie eine Mehrheit der Befragten (68 Prozent) ‚Social Scoring' wie in China ab. Die größten Gefahren sehen die Befragten darin, falsch bewertet zu werden, langfristige Stigmatisierung und in stärkerem Misstrauen in der Gesellschaft (Statista, 05.02.2019).

Wenn sich der Telematik-Trend durchsetzt, könnten sich in Zukunft risikobasierte Individualtarife am Markt etablieren und das Solidarprinzip aushebeln. Die Zunahme solcher Tarife könnte eine Marktdynamik auslösen und in Zukunft ein sozialer Zwang zur Datenpreisgabe entstehen. Persönliche Informationen über das Fahrverhalten werden dann zunehmend preisgegeben, um sich von anderen, schlechteren und damit risikoreicheren Fahrern, zu differenzieren. Die Folge wäre, dass diejenigen, die sich etwa aus Datenschutzgründen gegen Telematik-Tarife entscheiden, mehr zahlen müssten und diskriminiert würden. Besonders Telematik-Tarife, die Kriterien des Fahrstils und Verhalten des Fahrers messen und bewerten, bergen große Risiken für die Privatsphäre.

Profilbildung stellt einen Eingriff in die informationelle Selbstbestimmung dar. Eingeschränkt wird aber auch die persönliche Selbstentfaltung, denn die Daten basieren auf Verhalten in der Vergangenheit und können die Chancen für die Zukunft beeinflussen. Aufgrund der hohen Risiken sollten Telematik-Tarife reguliert und die Zulässigkeit von bestimmten Tarifgestaltungen gesetzlich verboten werden. Zumindest muss geregelt werden, wer, wie und wann Zugriff auf die Daten hat, wann diese gelöscht werden müssen und wie der Einzelne sich gegen ungerechtfertigte oder falsche Bewertungen wehren kann.

Auch wenn die Vorteile des vernetzten Autos groß sind, muss die Digitalisierung mit Augenmaß vorangetrieben werden. Das Auto darf dabei nicht zum totalen Überwacher des Fahrers und des Umfeldes werden. Jeder weitere Schritt in Richtung Vernetzung und Automatisierung bedarf einer umfassenden Datenschutz- und Risikofolgenabschätzung. Oder um es mit den Worten von Ulrich Kelber zu sagen: Auch ‚Autofahrer haben ein Recht auf digitale Unversehrtheit' (Tagesspiegel Background, 01.01.2019).

Über die Autorin

Marion Jungbluth
studierte Betriebswirtschaftslehre und Politologie, Soziologie und Psychologie. Nach mehrjähriger Tätigkeit als wissenschaftliche Mitarbeiterin von Bundestagsabgeordneten kam sie als wissenschaftliche Referentin im Bereich Klimaverträgliche Mobilität zum Verbraucherzentrale Bundesverband (vzbv). Von dort wechselte sie als Politische Referentin Nachhaltige Mobilität in die Abteilung Industrie-, Dienstleistungs- und Strukturpolitik des DGB-Bundesvorstands. Seit 2013 ist sie Leiterin des Teams Mobilität und Reisen beim vzbv, verantwortlich für die Themen Mobilität, Reisen und Ressourcenschutz. Sie vertritt den vzbv in diversen Stakeholder-Gremien wie zum Beispiel im Runden Tisch zum automatisierten und vernetzten Fahren, in der Nationalen Plattform Mobilität oder in der Initiative Digitale Vernetzung im Öffentlichen Personenverkehr.

Anzeige

RHENUS DATA OFFICE GMBH

RHENUS LOGISTICS

IHR PARTNER FÜR DATENSCHUTZGERECHTE AKTENVERNICHTUNG

OB AKTENORDNER, CDS, MIKROFICHE ODER MAGNETBANDSPEICHER...

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

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

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

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

DATENSCHUTZPRAXIS

ALS COMPLIANCE SCHOCKTE – EIN RÜCKBLICK AUF 2018

Dr. Niels Lepperhoff

Einleitung

2018 war ein einschneidendes Jahr verbunden mit vielfältigen, individuellen Erfahrungen aber auch Entwicklungen im Datenschutz. Ich möchte die Gelegenheit zu einem ganz persönlichen Rückblick und einem kleinen Ausblick nutzen.

Neue Kunden sind nicht immer wünschenswert

Je länger ich mich mit der DS-GVO beschäftigte, desto deutlicher schälten sich ihre vielen kleinen ineinander greifenden Rädchen heraus. Zwei dieser Rädchen, Rechenschaftspflicht und Bußgeldhöhe, entfalteten 2017/2018 eine überzeugende Wirkung. Die öffentliche Berichterstattung, die sich nicht immer von einer Hysterie unterscheiden ließ und selten von Sachkenntnis getrübt war, befeuerte die Panik. Erinnert sei an abgeschaltete Webseiten oder „das Ende der Fotografie“. Aus Angst fingen immer mehr Unternehmen, Vereine und öffentliche Stellen an, sich mit Datenschutz zu beschäftigen.

Fühlbares Zeichen des neuen Interesses am Datenschutz waren Anfragen nach einem Datenschutzbeauftragten (DSB). Bei uns sind im ersten Halbjahr 2018 sehr viele Anfragen eingegangen, ob wir als DSB zur Verfügung stünden. Schnell wurde vielfach klar, dass es sich um Verantwortliche handelt, die schon seit langer Zeit einen DSB gebraucht hätten. Der Plan des Gesetzgebers, den Anteil der Verantwortlichen zu erhöhen, die sich an das Datenschutzrecht halten wollen, ging ein Stück weit auf.

Mehr Kunden sind auf den ersten Blick sehr erfreulich, höre ich oft. Ja, das trifft für Gütergeschäfte zu. Vielfach beschlich mich der Eindruck, Anfragende wissen nicht, welche Art von Leistung sie mit „DSB“ einkaufen werden. Bei gängigen Dienstleistungen wie z.B. Steuerberatung ist in den Grundzügen bekannt, was ein Kunde beitragen sollte und welche Arbeitsergebnisse er erwarten kann. Da bereits die grundlegenden datenschutzrechtlichen Anforderungen an Unternehmen unbekannt sind, fällt es DSB suchenden Unternehmen schwer den eigenen Anpassungsbedarf abzuschätzen und die Arbeit eines DSB einzuordnen. Veränderungen sind nur dann erfolgreich, wenn die Unternehmensführung des Kunden eine Veränderung will und unterstützt. Irritationen auf beiden Seiten sind noch die mildeste Folge.

Der BvD e.V. engagiert sich an vielen Stellen, den Beruf des DSB bekannter zu machen. An dieser Stelle meinen ganz herzlichen Dank an alle Mitwirkenden! Doch werden wir als Berufsverband die tieferliegende Ursache nicht alleine beheben können.

Der Compliance Schock

Ein Blick in die Zahlen macht deutlich: Datenschutz geht noch lange nicht alle Unternehmen etwas an. Der BvD e.V. hat Datenschutzaufsichtsbehörden befragt, wie viele Datenschutzbeauftragte gemeldet worden sind. Für die folgende Berechnung durfte der Autor auf einen Zwischenstand zurückgreifen. Zwischenstand bedeutet, dass für fünf Bundesländer keine Angaben vorliegen. Der BfDI wird in der Auswertung nicht berücksichtigt, da er mit Blick auf die Privatwirtschaft nur eine ergänzende Rolle einnimmt.

Die gemeldeten Zahlen enthalten teilweise Datenschutzbeauftragte für private und öffentliche Stellen. Wo eine Trennung möglich war, wurden Datenschutzbeauftragte für öffentliche Stellen herausgerechnet. Weiterhin geben die Aufsichtsbehörden an, dass die Zahlen nicht um doppelte Meldungen bereinigt worden sind. Die Gesamtzahl von 140.059 überzeichnet deshalb die tatsächlichen Meldungen.

2017 (neuere Zahlen liegen nicht vor) waren 372.599[1] Unternehmen mit 10 und mehr sozialversicherungspflichtigen Beschäftigten bundesweit registriert. Das entspricht 11 % aller Unternehmen. Davon wurde die Anzahl an Unternehmen aus den Bundesländern abgezogen, für die keine Angaben zu Meldungen vorliegen. Herangezogen wurden dazu die Unternehmensregister der jeweiligen Landesstatistikämter soweit wie möglich für das Jahr 2017, sonst für das Jahr 2016. In Summe bleiben 291.040 Unternehmen übrig.

Unbeschadet anderer Kriterien hätte jedes dieser Unternehmen einen DSB bestellen müssen. Faktisch taten es nur 48 %. Die Zahl der Bestellungen sagt selbstverständlich nichts darüber aus, ob die übrigen Datenschutzvorschriften eingehalten werden.

Für Organisationen, die Daten bisher nach Gusto und Gefühl verarbeitet haben, ist es schockierend zu erfahren, dass Gesetze Grenzen setzen (Abbildung 1). „Warum brauche ich eine Rechtsgrundlage, die Daten haben wir doch schon?“, „Daten löschen geht nicht; wir wissen nicht, wozu wir die noch brauchen.“ Insofern spiegelte die öffentliche Berichtserstattung im Kern die Irritationen bei verantwortlichen Führungskräften wieder. Ein Unternehmen, das nach zehn Jahren die Buchführung und Steuererklärung „entdeckt“, wird ähnlich überrascht sein, welche Vorschriften das Handels- und Steuerrecht kennt. Auch, dass das Geld auf dem Konto teilweise dem Finanzamt zusteht…

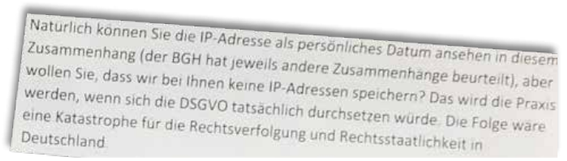

Natürlich können Sie die IP-Adresse als persönliches Datum ansehen in diesem Zusammenhang (der BGH hat jeweils andere Zusammenhänge beurteilt), aber wollen Sie, dass wir bei Ihnen keine IP-Adressen speichern? Das wird die Praxis werden, wenn sich die DSGVO tatsächlich durchsetzen würde. Die Folge wäre eine Katastrophe für die Rechtsverfolgung und Rechtsstaatlichkeit in Deutschland

Abbildung 1: DS-GVO als Gefahr für die Rechtsstaatlichkeit

Schockierte Personen brauchen persönliche Ansprache und Begleitung. Es reicht nicht ein Muster zum Ausfüllen zuzuschicken. Das Gegenüber möchte sich erst einmal ausweinen und weiß anschließend – auch beim besten Willen nicht – was das Muster von ihm will (Abbildung 2 zeigt die Kundenänderung im Muster einer Datenschutzinformation). Schon die Frage „Zu welchen Zwecken verarbeitet Ihre Abteilung personenbezogene Daten?“ überfordert viele Führungskräfte. Wie wird jemand, der bereits die zentrale Zweckfrage als eine Überforderung empfindet, auf die anderen Rädchen der DS-GVO reagieren? ▶

[1] DESTATIS (2018): Unternehmensregister, Stand 30.09.2018. URL: https://www.destatis.de/DE/ZahlenFakten/GesamtwirtschaftUmwelt/UnternehmenHandwerk/Unternehmensregister/Tabellen/UnternehmenBeschaeftigtengroessenklassenWZ08.html, Letzter Zugriff: 2019-01-19

DATENSCHUTZPRAXIS

Datenempfänger	Erläuterung
[illegible]	[illegible]
Erben	<Platzhalter, bitte erläutern was diese erhalten>Sterbegeld
[illegible]	[illegible]

Abbildung 2: Beispiel für ein Missverständnis bei einer Datenschutzinformation nach Artt. 13 und 14 DS-GVO

Überforderung für Geschäftsführer und Führungskräfte hinterlassen auch bei uns Spuren. Immer wieder aufs Neue zu erklären, dass der Kern des Datenschutzrechtes (Zweckbindung, Rechtsgrundlage, Löschpflicht) seit den 1970er Jahren besteht, stumpft ab. Intern lässt sich über das GAP zwischen Ist und Soll sprechen. Problematischer wird es, wenn nach außen kommuniziert werden muss, warum Praktiken mangels Rechtsgrundlage eingestellt werden. Auf die DS-GVO schieben funktioniert meistens nicht, da die Rechtsgrundlagen sich im Kern nicht geändert haben. Schnell würde auffallen, dass auch ein Verstoß gegen das BDSG-alt vorlag. Gut, dass die Verjährungsfrist des OWiG kurz ist.

Rechtsunsicherheit oder doch „Tool-Unsicherheit"?

Rechtsunsicherheit und DS-GVO wurden vielfach in einem Atemzug genannt. Neue Vorschriften werfen immer die Frage auf, wie sie zu interpretieren sind. Fehlt eine „dominierende" Interpretation – gefunden durch höchstrichterliche Rechtsprechung oder herrschende Literaturmeinung – eröffnen sich Freiräume. Diese lassen sich für Unternehmen fruchtbar machen. Fruchtbar machen bedeutet aber, dass es keine Checkliste gibt, die blind abgearbeitet werden kann. Es bleibt nur der mühevolle Weg sich ein Verständnis des Gesetzes selbst zu erarbeiten, bis erste Hilfestellungen aus juristischer Literatur und Rechtsprechung vorliegen.

Die Klage „Rechtsunsicherheit" verdeckt eine deutlich größere Unsicherheit: die „Tool-Unsicherheit". Mit Tool-Unsicherheit meine ich die Frage, wie lässt sich eine gesetzliche Anforderung praktisch umsetzen. Beispiele: Wie schreibe ich eine Datenschutzinformation nach Artt. 13 und 14 DS-GVO konkret? Wann ist eine AVV zu schließen? Wie motiviere ich die IT zu einem Sicherheitskonzept nach Art. 32 DS-GVO?

Warum ich die Datenschutzinformation als Beispiel für Tool-Unsicherheit aufführe, wenn es doch schon Generatoren im Internet gibt? Weil sie ein gutes Beispiel für das Ineinandergreifen der Rädchen ist. Der Wortlaut von Artt. 13 und 14 DS-GVO verleitet dazu, nur die Zwecke aufzunehmen, die häufig vorkommen. Bei einer Webseite wird dann das Ausliefern der Webseite, die eingebundenen Trackingtools und das Kontaktformular berücksichtigt. Klingt vollständig, wird aber im Alltag zu einer spannenden Situation führen, wenn ein Sicherheitsvorfall auftritt und die Logfiles nicht ausgewertet werden dürfen, weil gegen die Zweckbindung verstoßen würde. Eine Zweckänderung ist – wenn überhaupt – regelmäßig nur bei Kompatibilität zulässig (Art. 6 Abs. 4 DS-GVO). Deshalb empfiehlt es sich, alle Zwecke, für die absehbar die Daten verwendet werden sollen, zu nennen. Ich denke hier bspw. an die Wirksamkeitstests, Überwachung durch den DSB, Verfolgung von Regelverletzungen, Aufklärung, Meldung von Sicherheitsvorfällen, Prüfung durch Betriebsprüfer und zivilrechtliche Ansprüche.

Das Zusammentragen der Zwecke, die in größeren Unternehmen von ganz unterschiedlichen Personen verfolgt werden, ist die eigentliche Herausforderung. Die Pflege wird nicht minder herausfordernd. Es gilt Prozesse einzuführen oder zu ergänzen, so dass Änderungen von den einzelnen Beteiligten erkannt und gemeldet werden.

Ausblick 2019

Die Tool-Unsicherheit zeigt, dass wir bei der Frage, wie lassen sich die Anforderungen in Organisationen dauerhaft umsetzen, noch am Anfang stehen. Einerseits gilt es, das Verständnis der Anforderungen aus der DS-GVO auszubauen und diese Anforderungen in die Prozesse einzubauen. Dauerhaft lassen sich Datenschutzvorschriften nur dann verlässlich einhalten, wenn Compliance das Ergebnis aller Prozesse ist und keine „zusätzliche" Aktivität. Die eigentliche Herausforderung liegt deshalb nicht in der Rechtmäßigkeitsprüfung, sondern in der Gestaltung und Begleitung der organisatorischen Veränderungen.

Veränderungen kosten Kraft und brauchen Zeit. Fast möchte man begrüßen, dass 52 % der Unternehmen pflichtwidrig keinen DSB gemeldet – also vermutlich auch nicht benannt – haben. Die 48 % sind schon fordernd genug. Gegen diesen Gedanken spricht die Arbeitsteiligkeit unserer Wirtschaft. Daten fließen entlang der Lieferketten durch verschiedene Unternehmen. An den Schnittstellen zwischen den beteiligten Unternehmen wollen bspw. Zwecke und Rechtsgrundlagen abgestimmt werden. Manchmal muss sogar eine Auftragsverarbeitungsvereinbarung (AVV) geschlossen werden. Wenn alle Beteiligten die DS-GVO kennen und einhalten wollen, findet sich regelmäßig eine Lösung. Konflikte entstehen, wenn eine Seite keine Ahnung vom Datenschutzrecht hat oder dessen Anwendung verweigert (Abbildung 1).

Wenn ein Anbieter Passwörter unverschlüsselt speichert (und sich dann noch hacken lässt), obwohl seit Jahren eine gehashte, gesalzene und gepfefferte Speicherung Stand der Technik ist, sieht es vordergründig wie ein Einzelfall aus. Die bekannte Menge an illegal beschafften Login-Daten inkl. Passwort[2] weckt Zweifel am „Einzelfall". Von eigenen Erfahrungen aus Diskussionen mit Unternehmen hier ganz zu schweigen. Viele „Einzelfälle" lassen Vertrauen in Unternehmen und letztlich in unsere Gesellschaftsordnung erodieren.

Wer jetzt sagt, das regelt der Markt schon, macht es sich entschieden zu einfach. 52 % sind etwas mehr als die Hälfte aller Unternehmen. Wie soll die eine Hälfte der anderen ihren Willen aufdrücken? Ob die Situation in den übrigen EU-Mitgliedsstaaten und bei in der EU-tätigen Unternehmen aus Drittstaaten viel besser ist, darf bezweifelt werden. In der Praxis lassen sich u.U. keine DS-GVO konformen alternativen Anbieter finden. Die DS-GVO erfüllt den Datenschutzaufsichtsbehörden den Wunsch nach Rechenschaftspflicht und eigener Sanktionskompetenz. Nutzt diese Instrumente!

Ein wesentlicher Treiber ist die Angst vor hohen Bußgeldern. Sie steht in einem seltsamen Kontrast zur durchschnittlichen Bußgeldhöhe 2018. In NRW wurden bspw. durchschnittlich 455 Euro[3] pro Bescheid verhängt. Betriebswirtschaftlich verständlich wäre eine Entscheidung, das Datenschutzrecht zu ignorieren und das Bußgeld zu bezahlen. Ein DSB kostet auf jeden Fall mehr.

Die DS-GVO hat es geschafft, Datenschutz besser durchzusetzen. Es bleibt zu hoffen, dass dieser Erfolg nachhaltig sein wird. Auch wenn man über die eine oder andere Regelung geteilter Meinung sein kann, halte ich sie in Summe für einen Erfolg. Jetzt, wo ernsthaft erwogen wird, Datenschutzgesetze auch einzuhalten, kommt der Ruf nach Abschaffung. Verständlich, nicht befolgte Gesetzte tun nicht weh und demonstrieren doch politische Tatkraft. Dabei wird nicht nur verdrängt, dass Datenschutz Grundrechtsschutz, d.h. Demokratieschutz, ist. Erst wenn Datenverarbeitern durchgesetzte Schranken auferlegt werden, lässt sich langfristig Vertrauen von Bürgern in die Datenverarbeitung aufrechthalten und unsere Gesellschaftsordnung bewahren.

Über den Autor

Dr. Niels Lepperhoff

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

[2] Vgl. bspw. Heise Online (2019): Passwort-Sammlung mit 773 Millionen Online-Konten im Netz aufgetaucht, 17.01.2019, URL: https://www.heise.de/security/meldung/Passwort-Sammlung-mit-773-Millionen-Online-Konten-im-Netz-aufgetaucht-4279375.html, Letzter Zugriff 21.01.2019.

[3] Eigene Berechnung basierend auf Zahlen aus Handelsblatt (2019): Behörden verhängen erste Bußgelder wegen Verstößen gegen DS-GVO, 18.01.2019, URL. https://www.handelsblatt.com/politik/deutschland/Datenschutz-Grundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-DS-GVO/23872806.html, letzter Zugriff 2019-01-19

DATENSCHUTZPRAXIS

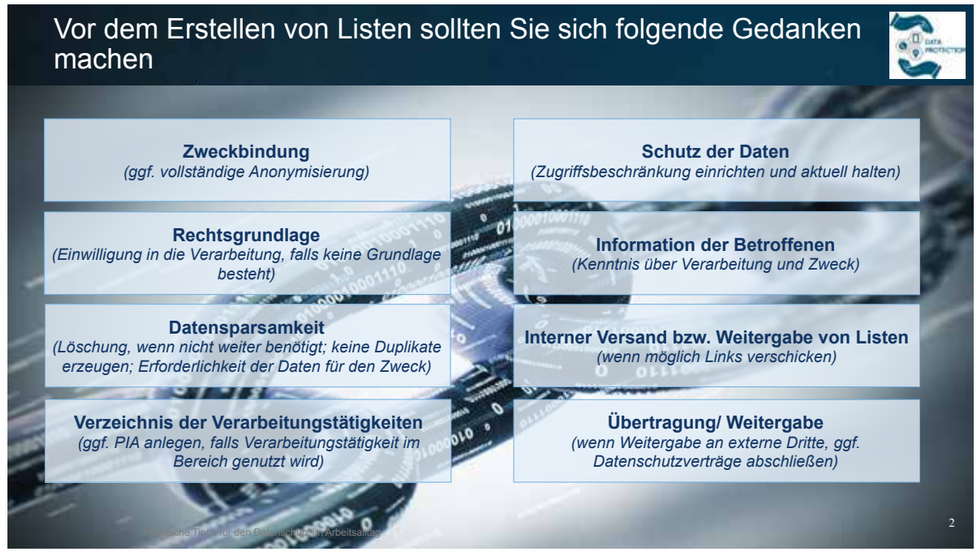
DIE UMSETZUNG DER DS-GVO IM UNTERNEHMEN – BERICHT AUS DER PRAXIS

Timo Ahland

DS-GVO im Unternehmen – der ideale Networking Faktor!

Neulich traf ich einen Kollegen aus der Abteilung der Medizindaten-Analysten, der seit Anfang 2017 als Koordinator seines Fachbereichs in unserem DS-GVO-Implementierungsprojekt mitarbeitet. Bei solchen Gelegenheiten bitte ich die Kollegen immer um Feedback, und er sagte ganz spontan: „So viele für mein Netzwerk im Unternehmen weiterführende Kontakte wie durch das DS-GVO-Projekt im letzten Jahr habe ich in den zehn Jahren davor nicht gewonnen – klasse, was für neue Möglichkeiten dadurch entstanden sind!"

Geht es Ihnen auch so? Ich habe den Eindruck, die Talsohle unseres DS-GVO-Implementierungsprojektes ist durchschritten. Die Botschaften sind offenkundig bei den Kollegen angekommen. Jetzt gilt es, das Momentum zu nutzen und die eingeschlagenen Pfade und erreichten Erfolge auszubauen. 2019 dürfte sicherlich das entscheidende Jahr dafür sein, ob die DS-GVO nachhaltig in den Unternehmen Wirkung entfaltet: Während es vor einem Jahr darum ging die Aufmerksamkeit der Kollegen zu erreichen und die Bereitschaft zu erzeugen, sich mit dem Thema DS-GVO und dem Check sowie der notwendigen Anpassung und Neuausrichtung der Geschäftsprozesse zu widmen, geht es in vielen Gesprächen jetzt darum, noch bestehende Unsicherheiten durch Beratung abzustellen und konkrete Fragen zu Problemen im Tagesgeschäft zu beantworten. Ein weiteres Phänomen der Post-DS-GVO-Ära sind die zahlreichen Mythen, die viele Kollegen tagtäglich anbringen: Von der These, dass ja seit der DS-GVO ohne Einwilligung gar nichts mehr an Datenverarbeitung zu machen sei, bis zu der Annahme, dass jegliche Excellisten nunmehr der Genehmigung durch den Datenschutzbeauftragten bedürften, ist Vieles dabei, was dringend der Entmystifizierung bedarf. Dabei helfen nach meiner Erfahrung in der täglichen Beratungspraxis wenige aber dafür gezielte Arbeitsmittel: eine Übersicht über die gängigen Rechtsgrundlagen des Art. 6 (bzw. Art. 9 DS-GVO für besondere Kategorien personenbezogener Daten) und als sozusagen zweite Seite ein und derselben Medaille eine Darstellung über die Informationspflichten. Zusätzlich haben wir auf einer Seite die in Art. 5 DS-GVO normierten Grundprinzipien Zweckbindung, Datenminimierung usw. nach dem hier abgebildeten Muster erstellt. Anhand derer können die Vielzahl der gängigsten Anfragen im Erstgespräch bereits kurz aufgenommen und eingeordnet werden.



In vielen Bereichen laufen gleichzeitig auch große und komplexe Digitalisierungsprojekte. Wir Datenschützer werden neben der Beratung zur Wahl der richtigen Rechtsgrundlage für die Datenverarbeitung und zu der praktischen Umsetzung der Informationspflichten, auch mehr und mehr gern und immer frühzeitiger eingebundene Berater für Konzepte von Privacy by Design für neue Geschäftsmodelle. Nicht zuletzt durch unsere DS-GVO-Projektarbeit haben wir einen profunden und tiefen Einblick in das Unternehmen erhalten. Wir können daher auch zu strategischen Aspekten zur passenden Corporate Governance und zur Steuerung für Geschäftsmodelle und –prozesse mit beraten. Im Angebot pragmatischer und lösungsorientierter Konzepte liegt neben dem oben beschriebenen Vorantreiben der Vernetzung der Kollegen ein weiterer messbarer Mehrwert, den wir Datenschützer im Unternehmen bieten können. Damit lässt sich auch bei bislang eher dem Datenschutz gegenüber zurückhaltenden Unternehmensverantwortlichen punkten.

Der Fortschritt ist spürbar und viele Kollegen anderer Unternehmen bestätigen diesen Eindruck: Wo vor einem Jahr noch starke Ablehnung herrschte und nur Probleme gesehen wurden, ist mittlerweile ein hohes Maß an Sensibilität und Verständnis für die Notwendigkeit die Verarbeitungstätigkeiten zu identifizieren, zu bewerten und zu dokumentieren getreten. Jetzt können wir die neu eingeführten Prozesse für Verarbeitungsregister, Datenschutz-Folgenabschätzung oder zur Meldung von Datenschutzvorfällen bald auf den Prüfstand stellen. Was läuft gut und was bedarf der Verbesserung? Wozu gibt es mittlerweile konkretere Handlungsempfehlungen der Aufsichtsbehörden wie der Datenschutzkonferenz (DSK) oder des Europäischen Datenschutzausschusses? Holen Sie zu diesen Fragen und ganz allgemein zur Zusammenarbeit mit dem Datenschutz das Feedback der Kollegen ein – vielleicht haben Sie ja auch schon zum Entstehen von Netzwerken beigetragen, aus denen viel Neues und Kreatives entstehen kann. Sprechen Sie Ihre Kollegen an!

Über den Autor

Timo Ahland
ist Volljurist und seit 2013 bestellter betrieblicher Datenschutzbeauftragter der deutschen Landesgesellschaft des international ausgerichteten Unternehmensverbandes Boehringer Ingelheim, dem größten familiengeführten forschenden Pharmaunternehmen mit Hauptsitz in Deutschland. Darüber hinaus koordiniert er für den Global Data Privacy Officer des Konzerns die Zusammenarbeit der Datenschutzbeauftragten und -experten in der Region Europa und ist mit seinem Team Teil der Task Force zur Vorbereitung des Unternehmensverbandes auf die DS-GVO.

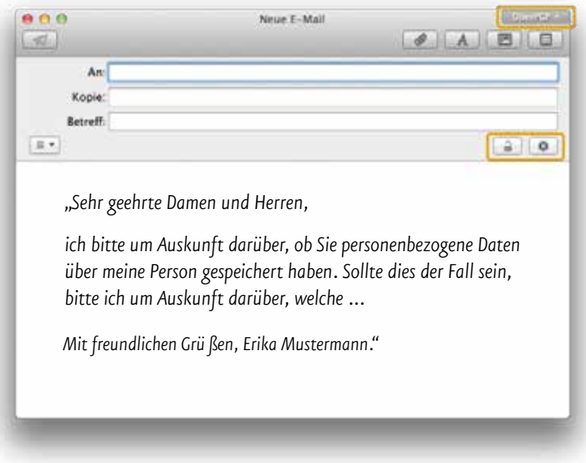
Boehringer Ingelheim

DATENSCHUTZPRAXIS

„EINE KURZE NACHFRAGE…“ – DS-GVO-KONFORME IDENTITÄTS-PRÜFUNG BEI DER ERFÜLLUNG VON BETROFFENENRECHTEN

Dr. Carlo Piltz und Melanie Pradel

Bing – eine neue E-Mail:



Manch einem stehen nach dem Lesen der ersten Zeilen dieser E-Mail die Schweißperlen auf die Stirn. Plötzlich fühlt man sich als Verantwortlicher hautnah den Anforderungen der DS-GVO ausgesetzt. Zudem besteht der Zeitdruck, Betroffenenanfragen grundsätzlich innerhalb eines Monats zu beantworten (Art. 12 Abs. 3 DS-GVO). Man bedenke nur die Sanktionsmöglichkeit der Aufsichtsbehörden, falls diese über eine unzureichende oder verspätete Auskunft an die betroffene Person informiert wird. Schnell hofft man auf eine negative Auskunftserteilung und sucht schon einmal den Namen im System: „Erika Mustermann“. Man bekommt eine Auflistung mehrerer Damen namens „Erika Mustermann“. Um welche Erika Mustermann muss man sich nun kümmern? Oder was passiert, wenn die in der Auskunft angegebenen Daten nicht mit den Daten im System übereinstimmen? Welche Frau Mustermann fragt an?

Nun vorschnell zu handeln, kann gravierende Konsequenzen nach sich ziehen. Insbesondere, wenn es sich um sensible Daten handelt, kann die Offenlegung gegenüber unberechtigten Dritten schwere Folgen für die betroffene Person selbst haben (z.B. bei Bank-, Zahlungs- oder Gesundheitsdaten). Auch bei der Ausübung der anderen Betroffenenrechte, wie dem Recht auf Löschung (Art. 17 DS-GVO) oder auch dem Recht auf Berechtigung (Art. 16 DS-GVO), muss der Verantwortliche sicherstellen, dass unberechtigten Dritten keine Daten zu einer anderen Person übergeben werden.

I. Pflicht zur Identitätsprüfung

Der Landesbeauftragte für Datenschutz und Informationsfreiheit in Baden-Württemberg (LfDI BaWü) rät deswegen dazu, vor der Durchführung der beantragten Maßnahmen eine eindeutige Identifizierung der betroffenen Person zu gewährleisten.[1] Die DS-GVO sieht in Art. 12 Abs. 6 DS-GVO eine Identitätsprüfung bei begründeten Zweifeln an der Identität der natürlichen Person, die den Antrag nach Art. 15 bis 22 DS-GVO gestellt hat, vor. Dies soll durch das Anfordern zusätzlicher Informationen, die zur Bestätigung der Identität der betroffenen Person erforderlich sind, geschehen. Wann allerdings von „begründeten Zweifeln“ auszugehen ist, darauf gibt die DS-GVO keine Antwort. Zudem spricht der Wortlaut „bei begründeten Zweifeln“ dem Anschein nach gegen eine grundsätzliche Pflicht zur Identitätsprüfung. Selbst die Datenschutzkonferenz nimmt zur Identitätsprüfung in ihrem Kurzpapier Nr. 6 lediglich wie folgt Stellung:

> *„Es muss sichergestellt werden, dass die zu beauskunftenden Daten nicht unbefugten Dritten zur Verfügung gestellt werden. Hierauf ist auch insbesondere bei mündlicher oder elektronischer Auskunftserteilung zu achten. Hat der Verantwortliche begründete Zweifel an der Identität eines Antragstellers auf Datenauskunft, so kann er nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen zur Bestätigung der Identität nachfordern (z. B. eine Postadresse bei elektronischem Auskunftsantrag)“.*[2]

II. Wann liegen „begründete Zweifel“ vor?

Gerade bei elektronischen Auskunftsverlangen ist davon auszugehen, dass allein die angegebene E-Mail-Adresse zur Identifizierung nicht ausreicht. Eine eindeutige Identifizierung kann in solchen Fällen meist nur durch ein bereits bestehendes Nutzerkonto beim Verantwortlichen mit einer bereits stattgefunden Verifizierung der E-Mail-Adresse garantiert werden.[3] Dennoch wird zum Teil davon ausgegangen, dass bei telefonischen oder elektronischen Auskunftsersuchen nicht von einer Pflicht zur Identifizierung auszugehen ist.[4] Es müssen dafür, nach dem Wortlaut der DS-GVO, „begründete Zweifel“ nachgewiesen werden, die dann vorliegen, wenn beispielsweise dem Verantwortlichen die E-Mail-Adresse oder die Anschrift der betroffenen Person nicht bekannt ist oder wenn die von der auskunftsersuchenden Person angegebene Adresse nicht mit der Adresse der betroffenen Person im Datenbestand des Verantwortlichen übereinstimmt.[5] Würde man dieser Ansicht folgen, bestünde aber in der Praxis ein reelles Risiko, unbefugt Daten an Dritte zu übergeben. Denn eine Webmail-Adresse ist heutzutage schnell durch jeden eingerichtet.

Mit dem 2. Datenschutz-Anpassungs- und Umsetzungsgesetz[6] (2. DSAnpUG) wurde bei bestimmten Auskunftsersuchen eine Identitätsprüfung bereits zwingend vorgeschlagen. Das Bundesmeldegesetz soll in § 10 Abs. 1 dahingehend geändert werden, dass vor Erteilung der Auskunft an die betroffene Person nach Art. 15 DS-GVO die Meldebehörde die Identität der betroffenen Person zu überprüfen hat.[7] Die Überprüfung beschränkt sich nicht nur auf elektronische oder telefonische Anfragen, sondern auf alle Formen der Geltendmachung des Auskunftsrechts.[8] Noch genauer soll die Identitätsprüfung bei Auskünften nach dem Nationalen Waffenregistergesetz (NWRG) geregelt werden. Gemäß dem angepassten § 19 NWRG ist die betroffene Person in der Pflicht, ihre Identität durch Vorlage einer amtlich beglaubigten Ausweiskopie oder einer amtlich beglaubigten Unterschrift nachzuweisen.[9] Begründete Zweifel bedarf es also nicht immer, sondern eine Identitätsprüfung kann bereits aufgrund der Sensibilität der personenbezogenen Daten und der Form des Anfrageweges als zwingend erforderlich angesehen werden. In solchen Fällen ist die Identitätsprüfung daher die Regel und nicht die Ausnahme.

Daneben sollte dann von „begründeten Zweifeln“ ausgegangen werden, wenn die Identität der auskunftsersuchenden Person nicht eindeutig durch Abgleich mit vorhandenen Daten geklärt werden kann. Auch dann bedarf es einer Identitätsprüfung, um nicht dem Risiko eines Gesetzesverstoßes (z.B. unzulässige Datenübermittlung an Dritte) ausgesetzt zu sein. Doch wie genau ist DS-GVO-konform eine solche Identitätsprüfung durchzuführen?

III. Möglichkeiten der Identifizierung

Der LfDI BaWü hat diesbezüglich Anfang Februar 2019 Stellung bezogen und Möglichkeiten zur „Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DS-GVO“[10] veröffentlicht. Generell wird aufgezeigt, wie der Verantwortliche bei einem Auskunftsersuchen oder auch bei der Ausübung anderer Betroffenenrechte im Hinblick auf die Identitätsprüfung vorgehen sollte. Grundsätzlich bestehen verschiedene Methoden zur Identifizierung der betroffenen Personen.

Die wohl gängigste und dem Wortlaut der DS-GVO entsprechende Methode, ist das **Abfragen zusätzlicher Informationen**. Dabei werden häufig die zusätzlich über Telefon oder auch per E-Mail erfragten Daten mit den in einer Datenbank vorhandenen Informationen abgeglichen. Das sind meistens die Adress- oder Geburtsdaten. Diese Methode wird vom LfDI BaWü nicht grundsätzlich infrage gestellt, dennoch sollte besondere Vorsicht walten, wenn es um die Auskunft sensibler Daten i.S.d. Art. 9 Abs. 1 DS-GVO geht. Der betroffenen Person nahestehenden Personen sind durchaus in der ▸

[1] Petrlic, Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO, DuD 1/2019, S. 1; abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/Identit%C3%A4tspr%C3%BCfung-bei-elektronischen-Auskunftsersuchen-nach-Art.-15-DSGVO.pdf.

[2] DSK, Kurzpapier Nr. 6 Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO, S. 2

[3] So Dehmel/Hullen, Auf dem Weg zu einem zukunftsfähigen Datenschutz?, ZD 2013, 147

[4] Paal/Hennemann, in: Paal/Pauly DSGVO BDSG, 2. Aufl. 2018, DS-GVO Art. 12 Rn. 72-74a.

[5] Bäcker, in: Kühling/Buchner DSGVO BDSG, 2. Aufl. 2018, DS-GVO Art. 12 Rn. 30.

[6] Deutscher Bundestag, BT Drs. 19/4674.

[7] BT Drs. 19/4674, S. 34.

[8] BT Drs. 19/4674, S. 222.

[9] BT Drs. 19/4674, S. 106

[10] Abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/Identit%C3%A4tspr%C3%BCfung-bei-elektronischen-Auskunftsersuchen-nach-Art.-15-DSGVO.pdf.

DATENSCHUTZPRAXIS

Lage, solche Identifizierungsfragen richtig zu beantworten. In solchen Fällen sollte, nach Ansicht der Aufsichtsbehörde, von dieser Methode nicht Gebrauch macht werden.

Eine andere gängige Form zur Identifizierung ist die **Übermittlung der Kopie eines Ausweisdokuments**. Datenschutzrechtlich mag das erst bedenklich klingen, aber die betroffene Person darf jene Daten, die nicht zur Identifizierung erforderlich sind, natürlich schwärzen und somit unkenntlich machen. Nach Auffassung des LfDI unterliegen die offengelegten Daten zudem einer strengen Zweckbindung und dürfen nur für die Identifikation selbst verarbeitet werden. Die postalische Übermittlung der Ausweiskopie zieht die Behörde der elektronischen Übermittlung vor, wobei letztere nur über einen sicheren Zugangsweg durchgeführt werden sollte. Dies muss der Verantwortliche beispielsweise durch eine Ende-zu-Ende-Verschlüsselung garantieren. Doch auch bei der Übermittlung von Ausweisdokumenten gibt der LfDI zu bedenken, dass der Zugang zu dem Ausweisdokument durch einen nahestehenden, aber unberechtigten Dritten nicht ausgeschlossen werden kann.

Eine weitere, aber noch durchaus unbekannte Möglichkeit, ist die I**dentifizierung über einen eIDAS-Dienst**. Das auf der EU-weiten eIDAS-Verordnung beruhende Verfahren ist ein elektronisches Identifizierungssystem, das in Deutschland bisher durch die Online-Ausweisfunktion des elektronischen Personalausweises und der sog. De-Mail umgesetzt wurde. Beide Verfahren basieren auf einer bereits durchgeführten Identitätsprüfung durch eine vertrauenswürdige Stelle, worauf sich der Verantwortliche im Rahmen seiner Prüfung berufen kann. Die Online-Ausweisfunktion wird zudem durch einen zusätzlichen PIN besonders geschützt.

Weiterhin ist eine **Identifizierung durch eine Post-/Video-Ident-Identifizierung** möglich. Im Rahmen des Post-Ident-Verfahrens wird bei einer Stelle der Deutschen Post durch einen Mitarbeiter die persönliche Identifizierung durchgeführt.

> *„Der Post-Mitarbeiter prüft dabei den Ausweis des anwesenden Antragstellers, fertigt eine Kopie davon an und leitet die Bestätigung der Identitätsfeststellung an den Verantwortlichen weiter, der die Identitätsfeststellung in Auftrag gegeben hat".*

Diese Methode wird heutzutage auch im Rahmen eines Video-Ident-Verfahrens angeboten. In solchen Fällen kommt es durch einen Video-Chat zur Identitätsüberprüfung, während dessen Aufnahmen der betroffenen Person und des Ausweises angefertigt werden. Beide Verfahren können im Auftrag des Verantwortlichen oder durch diesen selbst durchgeführt werden. Datenschutzrechtlich betrachtet, ist hier zwar keine Schwärzung des Ausweises möglich und auch die Datenschutzbestimmungen des Verantwortlichen sollten in diesem Fall ausreichend an die Aufnahmen angepasst sein. Dieser hohe Aufwand, auch von Seiten der betroffenen Person, geht aber nach Ansicht des LfDI mit einer ausreichend hohen Sicherheit bei der Identifizierung einher.

Die in der Praxis oft einfachste Umsetzung, um die Identität der betroffenen Person zu gewährleisten, ist die **Identifizierung über ein bestehendes Nutzerkonto** beim Verantwortlichen. Besteht ein solches bereits zum Zeitpunkt des Eingangs des Auskunftsersuchens, kam es bereits vorab zu einer digitalen Verifikation im Rahmen der Anmeldung. Jedoch weist der LfDI darauf hin, dass die eindeutige Identifizierung und die mit diesem Verfahren einhergehende Sicherheit auch von dem vom Nutzer selbst festgelegten Passwort abhängen.

IV. Fazit

Zwar besteht nach den Vorgaben der DS-GVO keine generelle Pflicht zur Identitätsprüfung. Dennoch sollte die Identität einer anfragenden Person in der Praxis nicht leichtfertig angenommen und im Zweifel lieber einmal mehr als einmal zu wenig nach zusätzlichen Daten gefragt werden. Über dem Verantwortlichen hängt hier stets das Damoklesschwert des Gesetzesverstoßes wegen einer unzulässigen Datenübermittlung an Dritte.

Um dieses Risiko zu minieren bzw. auszuschließen, ist es für Verantwortliche angebracht, im Vorhinein zu klären und intern Prozesse festzulegen, wie die Identitätsprüfung grundsätzlich durchzuführen ist. Nach Auffassung des LfDI darf dabei auch ein gewisser Aufwand von der betroffenen Person, wie bei der Video-Ident-Identifizierung, verlangt werden, um eine Identifizierung auch von Erika Mustermann zu gewährleisten.

Über die Autoren

Dr. Carlo Piltz

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

Melanie Pradel

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

▶ www.reuschlaw.de

reuschlaw
Legal Consultants

Anzeige

otris privacy
Konzerndatenschutz

Lückenlose Sicherheit im Datenschutz.

Durch die gezielte Umsetzung von Maßnahmen.

EU-DSGVO konform

otris software vereinfacht Verantwortung.

www.otris.de

ANFORDERUNGEN AN DIE DATENSCHUTZRECHTLICHE WIRKSAMKEIT DER EINWILLIGUNG

Prof. Dr. Jürgen Taeger

Verantwortliche, die personenbezogene Daten auf der Grundlage einer Einwilligung verarbeiten wollen, müssen sich mit den Anforderungen an eine wirksame Einwilligung vertieft auseinandersetzen, auch um kein Bußgeld nach Art. 83 Abs. 5 lit. a) DS-GVO zu riskieren. Erfolgt die Datenverarbeitung auf der Grundlage einer vor dem 25.5.2019 eingeholten Einwilligung, ist zu prüfen, ob diese Einwilligungen den Anforderungen der Art. 6 Abs. 1 UAbs. 1 lit. a, Artt. 7, 8 und 9 DS-GVO i.V.m. Art. 4 Nr. 11 DS-GVO genügen. Ist das nicht der Fall, müssen die Einwilligungen neu eingeholt werden.

Verbot mit Erlaubnisvorbehalt – Einwilligung als das Verbot legitimierende Erlaubnis

Nach Art. 8 Abs. 1 der Grundrechte der Europäischen Union (Grundrechte-Charta, GrCh) genießt jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden“ (Abs. 2). Festgeschrieben wird damit das „Verbot mit Erlaubnisvorbehalt“. Als Abwehr- und Schutzrecht verpflichtet die GrCh zu einer Gesetzgebung, die den Schutz der Persönlichkeitsrechte gewährleistet und die Erlaubnisse festlegt, nach denen personenbezogene Daten verarbeitet werden dürfen. Der EU-Gesetzgeber muss daher Sorge dafür tragen, dass das Grundrecht auf Datenschutz auch in Privatrechtsbeziehungen durch wirksame Regulierung Wirkung zeigt.

Auch nach dem aus Art. 2 Abs. 1 i.V.m. Art. 1 Grundgesetz abgeleiteten Recht auf Informationelle Selbstbestimmung durften personenbezogene Daten nur mit einer gesetzlichen Erlaubnis oder einer Einwilligung der betroffenen Person verarbeitet werden. Schon nach § 4 BDSG a.F. war die „Erhebung, Verarbeitung und Nutzung personenbezogener Daten … nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat“.

Aufgrund seiner grundrechtlichen Schutzpflichten hat auch der europäische Gesetzgeber seinen Ausgestaltungsauftrag, die Freiheitsrechte zu sichern, angenommen und mit der Europäischen Datenschutz-Grundverordnung (DS-GVO) ein in den Mitgliedstaaten unmittelbar geltendes Recht zum Schutz der Persönlichkeitsrechte bei der Verarbeitung personenbezogener Daten geschaffen. Die in Art. 5 DS-GVO enthaltenen allgemeinen Grundsätze des Datenschutzes sind Ausdruck dieses Verfassungsverständnisses, das auch den Verantwortlichen ausreichend Raum gewährt, ihre Grundrechte in einem fairen Ausgleich mit den Grundrechten der betroffenen (natürlichen) Personen zur Geltung zu bringen.

Ganz entsprechend wie vormals § 4 BDSG a.F. sieht nun Art. 6 DS-GVO vor, dass eine Verarbeitung nur rechtmäßig ist, wenn mindestens eine der in Art. 6 Abs. 1 UAbs. 1 DS-GVO genannten Bedingungen erfüllt ist. Ist das nicht der Fall, wäre noch zu prüfen, ob sich aus einer nationalen, aufgrund einer Öffnungsklausel der DS-GVO zulässigen oder nicht vom Anwendungsbereich der DS-GVO erfassten Datenschutzregelung eine Erlaubnis ergibt.

Erlaubnis der Datenverarbeitung aufgrund einer Einwilligung

Die Liste der sechs Erlaubnistatbestände des Art. 6 Abs. 1 UAbs. 1 DS-GVO wird von der Erlaubnis aufgrund einer Einwilligung angeführt. Daraus folgt keineswegs eine Rangfolge, sondern allenfalls wird damit das Selbstbestimmungsrecht besonders hervorgehoben und zum Ausdruck gebracht, dass die betroffene Person auch dann in freier Selbstbestimmung die Datenverarbeitung erlauben kann, wenn der Verantwortliche ansonsten keine gesetzliche Legitimation vorweisen kann. Die Erteilung einer Einwilligung ist demnach Grundrechtsausübung und keineswegs Grundrechtsverzicht. Beispielsweise darf darin eingewilligt werden, dass Daten aus einem Vertragsverhältnis auch für andere Zwecke, etwa das Marketing, verwendet werden. Selbst für die Persönlichkeitsrechte besonders riskante Verarbeitungen wie die von besonderen Kategorien personenbezogener Daten (Art. 9 Abs. 2 lit a) DS-GVO), eine ansonsten verbotene automatisierte Entscheidung im Einzelfall (Art. 22 Abs. 1 DS-GVO) oder die Übermittlung von Daten in ein Drittland, in dem es kein angemessenes Datenschutzniveau gibt (Art. 49 Abs. 1 lit. a DS-GVO), wird mit einer Einwilligung zulässig.

Aus der Sicht des Verantwortlichen empfiehlt es sich allerdings, zunächst nach einer gesetzlichen Erlaubnis zu suchen, auch weil eine Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann und sich der Verantwortliche damit auf unsicherem Terrain bewegt. Es ist auch dringend davon abzuraten, eine Einwilligung einzuholen, wenn ein gesetzlicher Erlaubnistatbestand vorliegt. Bei einem Widerruf der Einwilligung würde die betroffene Person kaum nachvollziehen wollen, wenn die Fortsetzung der Verarbeitung dann auf einen gesetzlichen Erlaubnistatbestand gestützt würde. Das ist zwar zulässig, wird in der Literatur aber auch unter Hinweis auf einen Verstoß gegen Treu und Glauben (§ 242 BGB) in Frage gestellt.[1]

Gesetzliche Anforderungen an die Wirksamkeit der Einwilligung

Will der Verantwortliche die Verarbeitung auf eine Einwilligung stützen, ergeben sich die Anforderungen an die wirksame Einwilligung aus einer Gesamtschau mehrerer Normen. Aus Art. 6 Abs. 1 UAbs. 1 lit. a und Art. 7 DS-GVO, der Definition der Einwilligung in Art. 4 Nr. 11 DS-GVO und den ErwG 32 f. und 42 f. ergeben sich die Anforderungen, nach denen die Einwilligung einer natürlichen Person in die Verarbeitung seiner personenbezogenen Daten, die ohne Einwilligung unzulässig wäre, wirksam ist.

Definition der Einwilligung in Art. 4 Nr. 11 DS-GVO

Zunächst ist die Definition der Einwilligung in Art. 4 Nr. 11 DS-GVO beachtlich. Dann enthält Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO den Erlaubnistatbestand der Einwilligung. Die näheren Anforderungen an die wirksame Einwilligung folgen sodann aus Art. 7 DS-GVO. Art. 8 DS-GVO enthält eine Regelung, wonach Kinder unter 16 Jahren die Zustimmung oder Einwilligung der Sorgeberechtigten benötigen, wenn Anbieter von sich an Jugendliche wendenden Telemedien Daten von Jugendlichen verarbeiten wollen.[2] Die Einwilligung in die Verarbeitung von besonderen Kategorien personenbezogener Daten behandelt Art. 9 DS-GVO. Außerhalb der DS-GVO enthält etwa § 26 Abs. 2 BDSG Hinweise darauf, unter welchen Voraussetzungen auch Beschäftigte in die Verarbeitung ihrer Daten durch den Arbeitgeber einwilligen können.

Nach Art. 4 Nr. 11 DS-GVO ist die Einwilligung von „der betroffenen Person“ selbst zu erteilen und „freiwillig“ und für einen bestimmten Verwendungszweck („für den bestimmten Fall“) auf der Grundlage ausreichender Informationen („in informierter Weise“) und „unmissverständlich“ entweder „in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung“ zu erteilen. Verlangt wird damit eine Erklärung oder Verhaltensweise, „mit der die betroffene Person in dem jeweiligen Kontext eindeutig ihr Einverständnis mit der beabsichtigten Verarbeitung ihrer personenbezogenen Daten ▸

[1] Näher dazu Taeger, in: Taeger/Gabel, DSGVO BDSG, Art. 7 Rn. 72 f.

[2] Siehe zu dem außerordentlich missglückten und zu zahlreiche Auslegungsfragen führenden Art. 8 DSGVO Taeger, in: Taeger/Gabel, DSGVO BDSG, Art. 8.

DATENSCHUTZPRAXIS

signalisiert“ (ErwG 32 Satz 1 und 1). Eine „konkludente Erklärung“ durch eine eindeutige und unmissverständliche Handlung ist möglich. Eine mutmaßliche Erklärung dagegen nicht. Schweigen oder Untätigkeit sind keine Handlungen. Nur dann, wenn besondere Kategorien personenbezogener Daten (z.B. Gesundheitsdaten) auf der Grundlage einer Einwilligung erhoben werden müssen, die betroffene Person „aus körperlichen oder rechtlichen Gründen [aber] außerstande ist, ihre Einwilligung zu geben“, darf zum Schutz lebenswichtiger Interessen der betroffenen Person eine Verarbeitung erfolgen (Art. 9 Abs. 2 lit. c DS-GVO).

Der Mitschnitt eines Telefonats – etwa in einem Callcenter zur Qualitätssicherung – ist nur dann zulässig, wenn die betroffene Person auf eine entsprechende Bitte um Zustimmung mit ‚ja‘ antwortet oder eine entsprechende Ziffer auf dem Telefon drückt.

Die Einwilligung der auf einem Foto in hervorgehobener Weise abgebildeten Person ist wegen des Bildnisschutzes aus § 22 Satz 1 KUG bei einem Verbreiten und öffentlich Zurschaustellen von Fotografien und Videoaufnahmen erforderlich, gleich ob man den § 23 KUG weiterhin für anwendbar hält oder dessen Inhalt bei der Abwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO berücksichtigt. Bei Aufnahmen von Personen (Erheben von Daten) sind die DS-GVO und das Allgemeine Persönlichkeitsrecht zu beachten.

Freiwilligkeit

Gemäß Art. 4 Nr. 11 DS-GVO muss die Einwilligung freiwillig erfolgen, was nach Art. 7 DS-GVO bedeutet, dass die Erklärung ohne jeden Zwang oder Druck abgegeben werden muss. Die betroffene Person darf keine Nachteile befürchten, wenn sie die Einwilligung versagt oder den Widerruf erklärt. Auf die betroffene Person darf kein emotionaler oder wirtschaftlicher Druck ausgeübt werden, um sie zu einer Einwilligung zu bewegen (Koppelungsverbot). Danach ist die Einwilligung nicht freiwillig, wenn ein Vertragsabschluss von der Einwilligung in die Verarbeitung solcher Daten abhängig gemacht wird, die für den Vertrag nicht erforderlich sind (ErwG 43).

An der Freiwilligkeit fehlt es, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht herrscht. Der Erwägungsgrund (ErwG) 43 geht davon aus, dass eine Behörde daher eine Verarbeitung im Rahmen ihrer Eingriffsverwaltung nicht auf eine Einwilligung stützen kann.

In der Leistungsverwaltung sehen das Gesetz zur Förderung der elektronischen Verwaltung (eGovernmentgesetz) des Bundes und inzwischen zahlreiche eGovG der Länder[3] vor, dass bei Durchführung eines elektronischen Verwaltungsverfahrens die vorzulegenden Nachweise elektronisch eingereicht werden können (§ 5 EGovG). Die zuständige Behörde kann die Nachweise auch direkt bei den ausstellenden Behörden dann einholen, wenn der Verfahrensbeteiligte darin eingewilligt hat (Abs. 2). In diesem Fall hat die Behörde sicherzustellen, dass die betroffene Person ihre Einwilligung bewusst und eindeutig erteilt hat, sie den Inhalt der zu protokollierenden Einwilligung jederzeit abrufen und sie jederzeit mit Wirkung für die Zukunft widerrufen kann.

Antragsverfahren sollen für Betroffene künftig noch weiter dadurch erleichtert werden, dass Anträge über einen Online-Service gestellt werden können, von denen die zur Antragstellung erforderlichen Dokumente bei Fachbehörden abgerufen und der für die Bescheiderteilung zuständige Verwaltungsbehörde zugeleitet werden können, wenn dafür die Einwilligung erteilt wird.

Zulässig sind Einwilligungslösungen zudem im Rahmen der Öffentlichkeitsarbeit einer öffentlichen Stelle, wenn um Aufnahme in den Verteiler von Pressemitteilungen oder von Informationsschriften ersucht wird. § 51 BDSG erhellt, dass im Anwendungsbereich dieser Vorschrift (Polizei und Justiz nach RL (EU) 2016/680) Einwilligungen nur zulässig sind, wenn dies nach einer Rechtsvorschrift ausdrücklich erlaubt ist.

Auch in einem sog. Subordinationsverhältnis wie zwischen Arbeitgeber und Beschäftigten (Legaldefinition in § 26 Abs. 8 BDSG) kann eine wirksame Einwilligung abgegeben werden.[4] Eine uneingeschränkte Ablehnung der Einwilligungsfähigkeit von Beschäftigten ist abzulehnen. So weit geht die strukturelle Unterlegenheit von Beschäftigten nicht, dass ihnen grundsätzlich, insbesondere nicht außerhalb der Bewerbungssituation, abgesprochen werden kann, frei und ohne Druck zu entscheiden, ob sie eine Einwilligungserklärung abgeben dürfen.[5] § 26 Abs. 2 Satz 1 BDSG stellt nun in Übereinstimmung mit ErwG 155 klar, dass eine Einwilligung im Beschäftigungsverhältnis möglich ist, und nennt in Satz 2 Beispiele für eine (freiwillige) Einwilligung im Beschäftigtenverhältnis.

Transparenz

Es gehört schon zu den Grundsätzen nach Art. 5 Abs. 1 lit. a DS-GVO, dass Betroffene die Verarbeitung ihrer Daten nachvollziehen können müssen. Das gilt besonders dann, wenn die betroffene Person mit ihrer Einwilligung eine Datenverarbeitung zulässig macht. Sie muss vor Abgabe ihrer Erklärung wissen, welche Daten zu welchem Zweck wie lange gespeichert werden, damit die Auswirkungen und damit die Tragweite der Einwilligung überblickt werden kann (informierte Einwilligung).

Zweckbindung

Die Einwilligung muss sich auf „einen oder mehrere bestimmte Zwecke“ beziehen (Zweckbindung). Ohne eine die Zweckänderung legitimierende erweiternde Einwilligung ist die zweckändernde Verarbeitung unzulässig. Eine Pauschal- oder Blankoeinwilligung ist unwirksam. Die Einwilligung kann befristet werden. Nach Fristende oder wenn der Zweck erfüllt ist, darf die Datenverarbeitung nicht mehr auf eine Einwilligung gestützt werden.

Der aufgrund der Öffnungsklausel in Art. 9 Abs. 2 lit. j DS-GVO zur Regelung befugte nationale Gesetzgeber sieht im BDSG eine Ausnahme von der strengen Zweckbindung für die wissenschaftliche, speziell die klinische Forschung vor, weil der konkrete Forschungszweck häufig bei der durch Einwilligung legitimierten Erhebung der Daten noch nicht benennbar ist („broad consent“, § 27 Abs. 1 BDSG). Das erkennt auch ErwG 33 an. Auf die Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung ist aber zu achten (§ 15 Abs. 3 MBO der Ärztinnen und Ärzte; Deklaration von Helsinki des Weltärztebundes). Weitere Anforderungen an die Einwilligung zur Teilnahme an einer klinischen Forschung folgen auch aus § 40 Arzneimittelgesetz (AMG). Die Einwilligung ist nach § 40 Abs. 2a Nr. 2 AMG teilweise unwiderruflich.

Form der Einwilligungserklärung

Die Einwilligung muss durch eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“ abgegeben werden. ErwG 32 erläutert dies näher und stellt klar, dass die Einwilligung durch eine bewusste und gewollte Handlung schriftlich, elektronisch oder mündlich abgegeben werden kann. Durch Schweigen oder Untätigkeit, etwa durch das Unterlassen des Entfernens eines voreingestellten Häkchens in einer Checkbox vor dem Text einer Einwilligungserklärung (opt-out), kann eine Einwilligung nicht erklärt werden – auch nicht nach ausdrücklichem Hinweis.

Eine höhere Anforderung an die Form der Einwilligungserklärung verlangt Art. 9 Abs. 1 DS-GVO bei einer Verarbeitung besonderer Kategorien personenbezogener Daten. Die Einwilligung muss dann „ausdrücklich“ erklärt werden (ErwG 51 Satz 6). Von Bedeutung ist hier auch Art. 2 Abs. 2 Nr. 21 der VO über klinische Prüfungen mit Humanarzneimitteln.

Die Einwilligung kann auch durch einen Boten überbracht werden. Selbst eine Stellvertretung soll dann möglich sein, wenn sich aus der Vollmacht ergibt, dass der Vertreter für bestimmte festgelegte Sachverhalte eine Einwilligungserklärung abgeben dürfe. Erfolgt die Verarbeitung aufgrund einer vom Stellvertreter abgegebenen Einwilligung, ist der Vertretene, die betroffene Person, darüber zu informieren, damit sie ggf. einen Widerruf erklären kann (Art. 7 Abs. 4 DS-GVO). Weil die Einwilligung eine höchstpersönliche Erklärung ist, bestehen aber Bedenken dagegen, dass ein Stellvertreter eine Einwilligung abgeben darf.[6]

Vorformulierte Einwilligungserklärungen sind zulässig, unterliegen aber dann als Allgemeine Geschäftsbedingungen der Inhaltskontrolle (§§ 305c, 307 Abs. 1 Satz 2 BGB). Wird die Einwilligungserklärung zusammen mit Erklärungen abgegeben, die auch andere Sachverhalte betreffen, so verlangt Art. 7 Abs. 2 DS-GVO, dass in dem vorformulierten Vertragsangebot „das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen [muss], dass es von den anderen Sachverhalten klar zu ▸

[3] In acht Bundesländern bestehenden kongruente Regelungen zum eGovG des Bundes oder Verweise auf die-ses; in den anderen Bundesländern liegen entsprechende Gesetzentwürfe vor oder es bestehen (noch) keine solche Regelungen.

[4] Zur Europarechtskonformität des § 26 BDSG etwa wg. des Erfordernisses der Schriftform für die Einwilligung Zöll, in: Taeger/Gabel, DSGVO BDSG, § 26 Rn. 72 ff.

[5] BAG K&R 2015, 433, m. Anm. Taeger, jurisPR-DSR 1/2015 Anm. 4.

[6] Vgl. Taeger, in: Taeger/Gabel, DSGVO BDSG, Art. 7 Rn. 9 ff.

unterscheiden ist“. Bei einem einseitigen Machtgefälle bestehen aber Bedenken gegen die formularmäßige Einwilligung. Das Bundesverfassungsgericht sieht das Recht auf Informationelle Selbstbestimmung verletzt, wenn in Versicherungsverträgen eine generelle Pflicht zur Schweigepflichtentbindung enthalten ist, um zu prüfen, ob ein Versicherungsfall vorliegt.

Einwilligung durch Jugendliche

Auch Jugendliche unter 18 Jahren (Minderjährige) können wirksam in die Verarbeitung ihrer Daten einwilligen, wenn im Einzelfall festgestellt wird, dass sie einsichtsfähig sind. Zu beachten ist aber, dass Anbieter von Diensten in der Informationsgesellschaft entweder eine Zustimmung der Sorgeberechtigten von Kindern, die das 16. Lebensjahr nicht vollendet haben, oder eine Einwilligung der Sorgeberechtigten benötigen, wenn der Anbieter die Vertragsdaten aus der Nutzung des Dienstes oder zusätzliche Daten verarbeiten will, die nicht für den Vertragszweck erforderlich sind (Art. 8 DS-GVO).

Widerruf der Einwilligung

Die Einwilligung kann ohne Angaben von Gründen mit Wirkung für die Zukunft ganz oder teilweise widerrufen werden (§ 7 Abs. 3 DS-GVO). So ist eine pauschale Einwilligung in die Verarbeitung zu Werbezwecken über alle Kommunikationskanäle lediglich hinsichtlich der Ansprache über Telefon widerrufbar. Die aufgrund einer Einwilligung verarbeiteten Daten sind, wenn nicht auch eine gesetzliche Erlaubnis vorliegt, ohne unangemessene Verzögerung zu löschen (Art. 17 Abs. 1 lit. b DS-GVO; ErwG 65 Satz 1). Eine seltene Ausnahme liegt vor, wenn die Daten unter dem Gesichtspunkt von Treu und Glauben (§ 242 BGB) nicht in zumutbarer Weise entfernt werden können.[7] An den Widerruf dürfen keine über die bei der Einwilligungserklärung gewählte Form hinausgehenden strengeren Anforderungen verlangt werden.

Dokumentation der Einwilligung

Der Verantwortliche muss für jede Phase der in der Legaldefinition des Art. 4 Nr. 2 DS-GVO genannten Verarbeitung und für jeden der mit der Verarbeitung verfolgten Zweck eine Erlaubnis haben und darüber auch in dem Verzeichnis der Verarbeitungstätigkeiten Rechenschaft ablegen (Accountability, Art. 5 Abs. 2, 30 DS-GVO). Die Beweislast für das Vorliegen einer Einwilligung vor Beginn der Verarbeitung – eine nachträgliche Legitimation durch Einwilligung ist nicht möglich – liegt bei dem Verantwortlichen, was bei konkludenten Einwilligungen eine herausfordernde Aufgabe ist. Dabei ist auch das Verfahren, wie die Erklärung zustande kam, zu protokollieren und zu dokumentieren. Auch die Angabe, welche Informationen über den Umfang und den Zweck der Datenverarbeitung sowie über das Widerrufsrecht der betroffenen Person gegeben wurden, ist festzuhalten. Damit soll einem um Auskunft bittenden Betroffenen die Selbstkontrolle ermöglicht werden; aber auch die Aufsichtsbehörde soll durch die Rechenschaftspflicht eine Unterstützung erhalten, wenn sie die Rechtmäßigkeit der Verarbeitung kontrolliert.

Rechtsfolgen der Missachtung der Anforderungen an eine Einwilligung

Gegen Verantwortliche, die etwa die Anforderungen an eine Einwilligung aus Art. 6 Abs. 1 UAbs. 1 lit. a DS-GVO sowie Art. 4 Nr. 11 und Art. 7 DS-GVO missachten, kann nach Art. 83 Abs. 5 lit. a DS-GVO ein Bußgeld verhängt werden. Die Geldbuße kann in sehr schweren Fällen bis zu 20 Mio. Euro oder 4% des gesamten weltweiten Jahresumsatzes des Unternehmens betragen.

Über den Autor

Prof. Dr. Jürgen Taeger

ist Direktor des Zentrums für Recht der Informationsgesellschaft (ZRI), Universität Oldenburg, und Of Counsel der internationalen Anwaltskanzlei DLA Piper am Standort Köln. Er ist Mitherausgeber des Großkommentars Taeger/Gabel, DSGVO BDSG, 3. Aufl., Frankfurt/M. 2019. Bei Fragen des Datenschutzes und der Compliance bei der Datenverarbeitung im Unternehmen und bei aufsichtsbehördlichen Verfahren unterstützt er mit seiner wissenschaftlichen Expertise.

Interdisziplinäres Zentrum für Recht der Informationsgesellschaft

DLA PIPER

[7] Dazu Taeger, jurisPR DSR 1/2015, Anm. 4.

Anzeige

DSGVO Praxisworkshops für Datenschutzbeauftragte.

Jetzt exklusive Praxis-Tipps sichern!

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

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

Ihre Vorteile im Überblick:

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

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

Wir freuen uns auf Ihre Teilnahme!

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

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

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

www.akademie.tuv.com

TÜVRheinland®
Genau. Richtig.

DATENSCHUTZPRAXIS

50-MIO.-EURO-STRAFE FÜR GOOGLE: EINE KRITISCHE BEWERTUNG DER BUSSGELDENTSCHEIDUNG DER FRANZÖSISCHEN DATENSCHUTZ-AUFSICHTSBEHÖRDE CNIL

Dr. Tilman M. Dralle

I. Einleitung

Am 21. Januar 2019 verhängte die französische Datenschutz-Aufsichtsbehörde CNIL ein Rekord-Bußgeld in Höhe von 50 Millionen Euro gegen Google. Grundlage der Bußgeldentscheidung sind von der CNIL festgestellte Verstöße gegen Artt. 6, 12 und 13 der DS-GVO im Zusammenhang mit der Verarbeitung personenbezogener Daten bei der Einrichtung eines Google-Accounts im Zuge der Konfiguration eines Mobiltelefons mit dem Android-Betriebssystem. So rügte die CNIL Mängel bei Form und Inhalt von Datenschutzhinweisen sowie unwirksame Einwilligungserklärungen in personalisierte Werbeanzeigen. Hintergrund des Verfahrens gegen Google sind Beschwerden zweier „Datenschutz-NGOs", NOYB und La Quadrature du Net, die unmittelbar nach Geltungsbeginn der DS-GVO bei der CNIL eingegangen waren.

II. Die CNIL-Entscheidung im Detail

Die Bußgeldentscheidung der französischen Aufsichtsbehörde ist deshalb von großer Bedeutung, weil sie eine erste Positionierung im Hinblick auf die komplexen Transparenzpflichten und Einwilligungserfordernisse der DS-GVO darstellt.

1. Informationspflichten

Die CNIL vertritt die Auffassung, dass die von Google zur Verfügung gestellten Informationen zur Datenverarbeitung entgegen der in Art. 12 DS-GVO geforderten „leicht zugänglichen Form" über mehrere Dokumente verteilt seien. Dies führe zu einer Fragmentierung von Informationen und zwinge die betroffene Person dazu, mit bis zu sechs Klicks verschiedene Dokumente aufzurufen und die darin enthaltenen Beschreibungen aufwändig zu vergleichen und einander zuzuordnen. Um beispielsweise zu erfahren, welche personenbezogenen Daten zur Anzeigenpersonalisierung verarbeitet werden, muss die betroffene Person zunächst den im Rahmen des Account-Erstellungsprozesses angezeigten Text „Datenschutz und Bedingungen" lesen. Dann muss die betroffene Person auf die Schaltfläche „Weitere Optionen" klicken, zum Abschnitt „Personalisierte Werbung" scrollen, den Link „Weitere Informationen" betätigen, die Overlay-Informationsbox mit dem Titel „Personalisierte Werbung" zur Kenntnis nehmen und als letzten Schritt den entsprechenden Abschnitt in der allgemeinen Datenschutzerklärung von Google konsultieren, die über einen Link im Text „Datenschutz und Bedingungen" aufgerufen werden kann.

Darüber hinaus stellt die CNIL Verstöße in Verbindung mit den materiellen Transparenzerfordernissen gemäß Art. 13 DS-GVO fest. So seien die in den Datenschutzhinweisen von Google genannten Zwecke (so z.B.: „Bereitstellung personalisierter Dienste, einschließlich Inhalte und Werbeanzeigen"; „Wir erheben Daten, um allen unseren Nutzern bessere Dienste zur Verfügung zu stellen […]. Welche Daten Google erhebt und wie diese verwendet werden hängt davon ab, wie Sie unsere Dienste nutzen und wie Sie Ihre Datenschutzeinstellungen verwalten.") zu generisch gehalten, um angemessen über Umfang und Konsequenzen der Datenverarbeitung zu informieren. Auch wenn aus Transparenzgründen nicht alle Details auf der ersten Ebene gestaffelt arrangierter Datenschutzhinweise enthalten sein sollten, so müsse Google bereits hier aussagekräftige Angaben machen, die es der betroffenen Person ermöglichen, Rückschlüsse über Anzahl und Umfang der Datenverarbeitungsvorgänge zu ziehen.

Darüber hinaus seien die Informationen bezüglich der Rechtsgrundlage für die Anzeigenpersonalisierung unklar bzw. missverständlich. So werde in den Datenschutzhinweisen einerseits darauf verwiesen, dass für personalisierte Werbung eine Einwilligung gem. Art. 6 Abs. 1 lit. a DS-GVO eingeholt werde („Wir ersuchen Sie um Ihre Einwilligung zur Verarbeitung Ihrer Daten für bestimmte Zwecke, und Sie haben das Recht, Ihre Einwilligung jederzeit zu widerrufen. Beispielsweise ersuchen wir Sie um Ihre Einwilligung, Ihnen personalisierte Dienste wie Werbeanzeigen bereitzustellen"). Andererseits würden auch die berechtigten Interessen Googles, gem. Art. 6 Abs. 1 lit. f DS-GVO, als Rechtsgrundlage für Werbemaßnahmen aufgeführt. Die betroffene Person könne daher nicht angemessen unterscheiden zwischen personalisierter Werbung, die auf einer (widerruflichen) Einwilligung basiert, und anderen, nicht-personalisierten Werbemaßnahmen, die auf Grundlage einer Interessenabwägung zulässig sind.

Außerdem seien die Informationen zur Dauer der Datenspeicherung teilweise unvollständig. So fehle für die in den Datenschutzhinweisen von Google genannte Kategorie „Daten, die über längere Zeiträume zu begrenzten Zwecken gespeichert werden" eine (präzise) Angabe der Dauer, für die die personenbezogenen Daten gespeichert werden, bzw. der Kriterien für die Festlegung dieser Dauer.

Screenshot 1: Abschnitt zur Speicherdauer von „Daten, die über längere Zeiträume zu begrenzten Zwecken gespeichert werden"

2. Einwilligung

Die CNIL führt in dem Bußgeldbescheid ferner aus, dass die von Google für personalisierte Werbung eingeholte „Einwilligung" nicht den Anforderungen der DS-GVO entspreche und damit nicht wirksam sei. Gemäß Art. 4 Nr. 11 DS-GVO ist eine Einwilligung „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist".

Screenshot 2: Per default angewähltes und ausgeblendetes Optionsfeld zur Anzeigenpersonalisierung

Erstens werde die Einwilligung in personalisierte Werbung nicht in informierter Weise abgegeben. Hier referenziert die CNIL die soeben ausgeführte Kritik an der Umsetzung der Informationspflichten. Außerdem verweist die CNIL darauf, dass Google lediglich über die Verarbeitung von Aktivitätsdaten in „Google services" für die Personalisierung von Werbung informiert, ohne diese „Google services" explizit und transparent zu benennen („Google can show you ads based on your activity on Google services (such as Search or YouTube), and on websites and apps that partner with Google").[1]

Zweitens werde die Einwilligung nicht für den bestimmten Fall und nicht unmissverständlich abgegeben. Da das Optionsfeld zur Einwilligung in die Anzeigenpersonalisierung bereits vorausgewählt sei (Opt-out), könne dies keine wirksame Einwilligung darstellen (Erfordernis der Unmissverständlichkeit). Darüber hinaus liege auch deshalb keine ▸

[1] Die von Google genutzte deutsche Formulierung („Google kann Ihnen Werbung auf der Grundlage Ihrer Aktivitäten zeigen. Die Werbeanzeigen erscheinen in Google-Diensten wie der Google-Suche oder YouTube sowie auf Partnerwebsites und in Partner-Apps") schafft (noch) weniger Transparenz als die englische Version, da in der deutschen Formulierung nicht die extensive Datenerhebung, sondern vielmehr die Anzahl der „Schaltflächen" für die personalisierte Werbung in den Vordergrund gerückt wird.

DATENSCHUTZPRAXIS

DS-GVO-konforme Einwilligung vor, weil das Optionsfeld standardmäßig ausgeblendet sei und daher keine auf einen bestimmten Zweck bezogene Willensbekundung bestehe (Erfordernis der Bestimmtheit). Vielmehr werde dem Benutzer mit Klick auf den Button „Konto erstellen" eine Art „Generaleinwilligung" abverlangt.

Dass Google nach dem Klick auf „Konto erstellen" ein Pop-Up einblendet, das auf die Anzeigenpersonalisierung hinweist und die betroffene Person zwischen „Weitere Optionen" und „Bestätigen" wählen lässt, heilt nach Ansicht der CNIL weder die fehlende Unmissverständlichkeit noch die fehlende Bestimmtheit der Einwilligung.

Screenshot 3: Pop-Up mit „Last-Minute-Hinweis" auf Anzeigenpersonalisierung

III. Bewertung

1. Informationspflichten

Der Tenor der CNIL-Entscheidung hinsichtlich der Fragmentierung von Informationen ist zu begrüßen. Über zahlreiche Dokumente verstreute Angaben zur Datenverarbeitung führen nicht zu Transparenz, sondern stiften eher Verwirrung. Grundsätzlich steht dies einer gestaffelten Informationsaufbereitung nicht entgegen. Allerdings sollten die in Schichten arrangierten Informationen von einem zentralen Punkt aus und mit wenigen Klicks zugänglich sein.

Die von der CNIL geäußerte Kritik an den Angaben zu Zwecken, Rechtsgrundlagen sowie der Dauer der Datenspeicherung ist hingegen zu hinterfragen. Wenn die CNIL beispielsweise die Zweckbeschreibung „Bereitstellung personalisierter Dienste, einschließlich Inhalte und Werbeanzeigen" als zu generisch kritisiert (wohlgemerkt: lediglich eine Überschrift (!) in Googles Datenschutzerklärung), stellt sich die Frage, (i) wie eine DS-GVO-konforme Zweckbeschreibung nach Auffassung der CNIL auszusehen hat und (ii) warum die CNIL die nachgelagerte, detailliertere Beschreibung personalisierter Werbeanzeigen einfach unter den Tisch fallen lässt.

Bei den Rechtsgrundlagen stellen sich ähnlich gelagerte Fragen. Zunächst einmal lässt sich der Datenschutzerklärung von Google entnehmen, dass die betroffene Person für die Bereitstellung *„[personalisierter]* Dienste wie Werbeanzeigen" um eine widerrufliche Einwilligung ersucht wird,[2] wohingegen (andere) Verarbeitungen zu Werbezwecken („Marketing, um Nutzer über unsere Dienste zu informieren" & „Werbung, um viele unserer Dienste Nutzern kostenlos zur Verfügung stellen zu können") auf einer Interessenabwägung basieren. Eine durchschnittlich verständige betroffene Person wird hieraus den Schluss ziehen können, dass für personalisierte Werbemaßnahmen ausschließlich die Einwilligungserklärung als Rechtsgrundlage fungiert, obgleich diese eine Teilmenge von allgemeinen Werbemaßnahmen darstellen. Bei jeder Rechtsgrundlage explizite Abgrenzungen zu anderen Rechtmäßigkeitstatbeständen vorzunehmen, ist zwar theoretisch möglich, wird praktisch aber durch den zwangsläufig steigenden Umfang und die Komplexität entsprechender Informationen dem Ziel der DS-GVO (und der CNIL), ein „Mehr" an Transparenz zu schaffen, kaum gerecht.

Auch bei den Ausführungen der CNIL zu den ihrer Meinung nach unpräzisen Angaben zur Dauer der Datenspeicherung lohnt sich ein kritischer Blick. Zwar findet man in den Datenschutzhinweisen tatsächlich keine Referenz auf ein bestimmtes Gesetz (wie „HGB") oder eine bestimmte Anzahl an Jahren (wie „10 Jahre"). Auf der anderen Seite wird bspw. auf „[steuerrechtliche] oder [buchhalterische]" Gründe für eine längere Datenspeicherung verwiesen. Fraglich ist, ob aufgrund der Vielzahl an möglichen Transaktionen und betroffenen Jurisdiktionen tatsächlich eine transparente Angabe einschlägiger Gesetze sowie der Dauer gesetzlicher Aufbewahrungspflichten möglich ist bzw. welche Anforderungen die CNIL in diesem Zusammenhang überhaupt stellt.

2. Einwilligung

Die Entscheidung der CNIL hinsichtlich der Wirksamkeit der eingeholten Einwilligung ist weitgehend nachvollziehbar. Das standardmäßig angewählte Optionsfeld „Personalisierte Werbung einblenden" kann nicht die Basis für eine unmissverständlich abgegebene Willensbekundung sein.[3] Dies gilt insbesondere, da den betroffenen Personen durch die standardmäßige Ausblendung ihrer Wahlmöglichkeiten von Google ein Wille unterstellt wird, der so ggf. gar nicht vorliegt. All dies führt richtigerweise zur Unwirksamkeit der Einwilligung. Denn die betroffene Person wird durch das geschickte Design des Account-Erstellprozesses dazu verleitet, per Klick auf das Pflichtfeld „Ich willige in die oben beschriebene Verarbeitung meiner Daten ein" eine bzw. mehrere Einwilligungen zu geben, deren Zweck bzw. Zwecke ihr nicht bekannt sind. Das nachfolgend eingeblendete Pop-Up ist nicht viel mehr als ein datenschutzrechtliches Feigenblatt.

Das Google eine Einwilligung auch DS-GVO-konform abfragen kann, zeigt das Beispiel der Sprach- und Audioaktivitäten. Diese können von Google aufgezeichnet werden, damit – so die Zweckbeschreibung – die „Stimme besser erkannt und die Spracherkennungsfunktion optimiert werden kann". Wie bei der Anzeigenpersonalisierung basiert die Datenverarbeitung hier laut der Google-Datenschutzerklärung auf einer Einwilligung. Allerdings ist in diesem Fall das Optionsfeld „Sprach- und Audioaktivitäten in meinem Google-Konto speichern" nicht standardmäßig angewählt. Die unterschiedliche Behandlung der beiden Einwilligungsszenarien verdeutlicht Googles Bestreben, zur Sicherung der Werbeeinahmen eine möglichst hohe Einwilligungsrate bei Anzeigenpersonalisierung zu erzielen, wenn nötig auch auf Kosten des Datenschutzes.

IV. Ausblick

Die Bußgeldentscheidung der französischen Datenschutz-Behörde CNIL ist ambivalent zu bewerten. Positiv ist die klare Positionierung hinsichtlich der Einwilligung: Nur ein unmissverständliches „Opt-In" in Form einer informierten Entscheidung genügt den Anforderungen der DS-GVO. Die sehr strenge Auslegung der Informationspflichten lässt hingegen einige Fragen offen. Denn legt man die von der CNIL angewandten Maßstäbe auch bei anderen Unternehmen in der Europäischen Union an, wird das Ergebnis in fast allen Fällen „non-compliance" sein.[4] Jeder Praktiker weiß: Wer (hier) sucht, der findet! Gerade für kleine und mittlere Unternehmen wären Kosten und Aufwand ab einem bestimmten Punkt nicht mehr verhältnismäßig. Eine Lösung könnte sein, die aus Artt. 13, 14 DS-GVO erwachsenden Pflichten „dynamisch" anzuwenden. Unternehmen, die Datenverarbeitungen mit hohen Risiken für die „Rechte und Freiheiten natürlicher Personen" betreiben (wie z.B. Google), müssten deutlich mehr leisten in puncto Transparenz als KMUs, die unbedenkliche Datenverarbeitungen in beschränktem Umfang vornehmen. Dieser Ansatz, der auch in der CNIL-Entscheidung anklingt, ist einerseits attraktiv, weil er risikobasiert ist und Verhältnismäßigkeitsgesichtspunkte integriert. Andererseits findet er keine (explizite) Grundlage im Wortlaut der Artt. 12 bis 14 der DS-GVO und birgt eine nicht zu unterschätzende Rechtsunsicherheit für betroffene Unternehmen. Eine erste Klärung dieses und anderer Aspekte der CNIL-Entscheidung wird durch die französische Verwaltungsgerichtsbarkeit und den Europäischen Gerichtshof (EuGH) erfolgen, da Google den Bußgeldbescheid derzeit gerichtlich überprüfen lässt.

Über den Autor

Dr. iur. Tilman M. Dralle, LL.M. (Nottingham)

Security Consultant mit den Schwerpunkten IT-Compliance, Datenschutz und Informationssicherheit bei TÜV Rheinland

TÜVRheinland®
Genau. Richtig.

[2] Hervorhebung durch den Autor.

[3] Siehe dazu auch Erwägungsgrund 32: „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person sollten … keine Einwilligung darstellen."

[4] Siehe hierzu auch Wybitul, „Französische Datenschützer verhängen Bußgeld gegen Google – Die Datenschutzdiskussion ist eröffnet", LTO, 24.1.2019, <https://www.lto.de/recht/kanzleien-unternehmen/k/datenschutz-dsgvo-verstoss-frankreich-google-bussgeld-zustaendigkeit-namentliche-nennung/>.

DATENSCHUTZPRAXIS

SIND PRIVATE MESSENGER-DIENSTE FÜR DIE UNTERNEHMENSINTERNE KOMMUNIKATION UNTER MITARBEITERN GEEIGNET?

Lena Bäumges

Die Qualität der internen Kommunikation in Unternehmen gewinnt immer mehr an Bedeutung. Unter Qualität werden die Relevanz der bereitgestellten Inhalte sowie die Art und Weise verstanden, wie diese Inhalte an verschiedene Mitarbeitergruppen übermittelt werden und wie die Empfänger untereinander – auch gruppenübergreifend – kommunizieren.

Die Mitarbeiter eines Unternehmens möchten sich miteinander vernetzen. Es ist daher nicht verwunderlich, dass sie dies anhand der sozialen Medien und Instant-Messaging-Dienste tun, die sie privat nutzen, wenn keine adäquate Alternative bereitgestellt wird. **90 % der deutschen Internetnutzer (62,4 Millionen) setzen Messenger-Dienst ein, 50 Millionen (81 %) nutzen WhatsApp und 28 Millionen (46 %) verwenden Facebook-Messenger[1].**

Studien besagen, dass zwei Drittel der Unternehmen in Deutschland ihren Mitarbeitern für die interne Kommunikation keine sichere Alternative zu den sozialen Medien zur Verfügung stellen. So entsteht schnell eine Schatten-IT im Unternehmen, denn 49 % der Beschäftigten haben WhatsApp auf ihren geschäftlichen Smartphones installiert.

Erschreckend daran ist, dass jeder Zweite sich darüber im Klaren ist, dass die Nutzung von WhatsApp und Co. zu beruflichen Zwecken datenschutzrechtliche Probleme für den Arbeitergeber mit sich bringen kann. 45 % von ihnen haben die App trotzdem auch für dienstliche Zwecke installiert. Außerdem nutzen laut einer Studie von Speakap[2] 47 % der Mitarbeiter[3] die sozialen Medien, um mit Kollegen, Managern und der Unternehmenszentrale zu kommunizieren.

Sicherheits- und Datenschutzprobleme stellen wohl das größte Risiko dar. Daher widme ich mich in den folgenden Abschnitten den Gefahren, die mit der Nutzung von privaten Messenger-Diensten im Unternehmen einhergehen.

WhatsApp greift z. B. regelmäßig auf alle auf dem Smartphone gespeicherten Kontakte zu, um zu prüfen, wer über den Dienst erreichbar ist. Alle Telefonnummern werden somit an WhatsApp weitergeleitet, unabhängig davon, ob die Inhaber den Dienst selbst nutzen oder nicht. Jeder Benutzer stimmt diesem Vorgang während der Installation zu. Doch wie hoch ist der Anteil derer, die die Nutzungsbedingungen von A bis Z durchlesen? Und was ist mit den Kontakten, die selbst kein WhatsApp nutzen?

Erstes Urteil

Das Amtsgericht Bad Hersfeld hat vor einiger Zeit in einem Beschluss entschieden, dass die Einwilligung aller Kontakte zur Nutzung des Dienstes und der damit verbundenen Datenweitergabe eingeholt werden muss. Hier liegt eine weitere Problematik. Zum einen werden personenbezogene Daten Dritter ohne deren ausdrückliche Genehmigung gegenüber dem Dienst erhoben, gespeichert und verwertet. Und zum anderen macht WhatsApp seine Benutzer mittels ihrer Zustimmung zu den Nutzungsbedingungen für die Weitergabe von personenbezogenen Daten Dritter verantwortlich.

Seit einiger Zeit gibt es in den Smartphone-Einstellungen die Option, WhatsApp den Zugriff auf Kontakte zu verbieten. Was geschieht jedoch mit den Daten, die vorher bereits verwendet wurden? Was passiert, wenn ein Handy an einen neuen Mitarbeiter übergeben wird, ohne dass die alten WhatsApp-Kontaktdaten gelöscht wurden? Und was ist, wenn ein Kollege keinen Gebrauch von der Option macht, weil er WhatsApp für seine privaten Kontakte nutzen möchte?

So würde beispielsweise ein Handwerker einen bußgeldbewehrten Verstoß gegen die DS-GVO begehen, wenn er Fotos von zu reparierenden Stellen einer Privatwohnung eines Kunden macht und diese an den Meister im Betrieb schickt, um sich mit ihm zu beraten. Hier muss er den Kunden vorab um schriftliche Einwilligung bitten. Ein solches Vorgehen ist undenkbar und bringt zu viel Bürokratie in die Digitalisierung.

Sammlung von Daten und Ende-zu-Ende-Verschlüsselung

Trotz DS-GVO tauscht WhatsApp auch in Europa weiterhin Daten seiner Benutzer mit der Muttergesellschaft Facebook aus[4]. Das Sammeln von Daten außerhalb des Facebook-Netzwerks wurde nun vor kurzem durch das Bundeskartellamt verboten. Facebook hat zwölf Monate Zeit, sein Verhalten zu ändern, und muss innerhalb von vier Monaten Lösungsvorschläge unterbreiten. Facebook gab bereits bekannt, dass es sich gegen das Votum wehren wird. Eine Änderung der plattformübergreifenden Sammlung von Daten in naher Zukunft ist also nicht in Sicht. Und wer weiß schon, wie zufriedenstellend die Lösung für den Datenschutz nach zwölf Monaten wirklich sein wird?

Auch die kürzlich bekanntgegebenen Pläne hinsichtlich der Fusion der Chat-Funktionen von Facebook-Messenger, WhatsApp und Instagram machen die Sachlage nicht angenehmer. Benutzer sollen dienstübergreifend chatten können, wobei die Ende-zu-Ende- Verschlüsselung für alle drei Dienste gegeben sein soll. Wie sicher die Daten jedoch sein werden, ist fraglich, da der Konzern natürlich mit allen Diensten anhand personalisierter Anzeigen Geld verdienen möchte. Diese Art der mobilen Werbung macht mittlerweile 93 % des Gesamtumsatzes aus[5].

„Diejenigen, deren Aufgabe es ist, den Benutzer

Foto: ink Drop / Shutterstock.com

zu schützen, führen immer einen harten Kampf gegen diejenigen, deren Aufgabe es ist, Geld für das Unternehmen zu verdienen“, kommentierte Sandy Parakilas, die bei Facebook im Bereich Privatsphäre tätig war, gegenüber der New York Times.

Hinzu kommt, dass WhatsApp und Facebook US-amerikanischen Recht unterliegen. Laut Patriot Act können US-Behörden ohne richterlichen Beschluss Dienste dazu auffordern, personenbezogene Daten freizugeben. Das bedeutet, dass verschlüsselte Daten entschlüsselt werden müssen. Dies gilt natürlich gleichermaßen für Dienste wie Skype oder Microsoft Teams. Auch hier verlassen sensible Daten Europa und landen auf US-amerikanischen Servern, wo sie dem Zugriff der US-Behörden ausgesetzt sind. Auch hier ist das Maß der Verschlüsselung der übermittelten Daten unklar, da die Details meist völlig intransparent sind und die Verschlüsselungshoheit in der Regel beim Anbieter liegt.

Was Mitarbeiter wirklich wollen

Die oben genannten Zahlen belegen die wachsende Beliebtheit von Messaging-Diensten trotz der Bedenken hinsichtlich des Datenschutzes in Unternehmen. Ob diese Dienste für den professionellen Einsatz in Unternehmen geeignet sind, ist eine andere Frage.

In einer kürzlich veröffentlichten Speakap-Studie[6] wurden die Teilnehmer (über 1.000 in verschiedenen Branchen tätige Mitarbeiter) gebeten, anzugeben, welche Funktionen für sie ▶

[1] https://www.messengerpeople.com/de/facebook-messenger-nutzerzahlen-deutschland-2018/

[2] https://www.speakap.com/de/

[3] https://resources.speakap.com/de/bridging-internal-communications-gap

[4] https://www.techbook.de/easylife/whatsapp-daten-facebook-dsgvo

[5] https://de.statista.com/infografik/1293/umsatz-von-facebook-nach-segmenten/

[6] https://resources.speakap.com/de/bridging-internal-communications-gap

bei der Verwendung von Mitarbeiter Apps oder Plattformen für die interne Kommunikation am wichtigsten sind:

- Übersichtliche persönliche Chronik (relevante Informationen für jeden Benutzer, entsprechend seiner Funktion)
- News-Beiträge
- Organisationsgruppen
- Dateimanagement
- Private Chats

Dies sind die fünf am meisten gewünschten Funktionen. Die Einführung eines reinen Messenger-Dienstes kann daher eine Mitarbeiter App nicht ersetzen. Immerhin ist der Bedarf einer übersichtlichen Chronik das am häufigsten verlangte Merkmal. Nach der Implementierung eines bloßen Messenger-Dienstes würde daher zum einen weiterhin betriebsintern über die öffentlichen sozialen Medien (aufgrund fehlender Chronik im bloßen Messenger) kommuniziert werden, und datenschutzrechtliche Risiken würden bestehen bleiben. Zum anderen sind die Newsfeeds oder Timelines oftmals voll von irrelevanten Nachrichten, die nicht den Interessen der Mitarbeiter in dem jeweiligen Bereich entsprechen. Hinzu kommt, dass die Chats schnell unübersichtlich werden, wenn z. B. themenübergreifend in einer WhatsApp-Gruppe kommuniziert wird. Die resultierende Informationsflut kann bei der Suche nach einer bestimmten Nachricht oder einem freigegebenen Dokument frustrierend sein.

Unternehmen haben zudem keine Kontrolle und keinen Einfluss darauf, wer in welchen WhatsApp-Gruppen Mitglied ist. Gruppen werden zumeist von Mitarbeitern gegründet, und Personen außerhalb des Unternehmens können unbemerkt hinzugefügt werden. Zudem arbeiten Unternehmen oft mit externen Parteien (Freiberufler, Partner, Lieferanten etc.) zusammen. Es ist naheliegend, dass diese auch in unternehmensinterne WhatsApp-Gruppen eingeladen werden. Nach der Beendigung des Projekts werden sie womöglich nicht wieder aus der Gruppe entfernt. Auch ehemalige Mitarbeiter werden nach ihrem Ausscheiden aus dem Unternehmen häufig in Gruppen vergessen. Dies kann besonders nachteilig werden, wenn sie und das Unternehmen im Streit auseinander gegangen sind.

Fazit

Spätestens seit der Einführung der DS-GVO ist es wichtig, dass Unternehmen eine klare Entscheidung darüber treffen, ob die Nutzung von privaten Messenger-Diensten und öffentlichen sozialen Medien zu dienstlichen Zwecken weiterhin gestattet oder toleriert wird. Einige Unternehmen haben bereits auf diese Problematik reagiert. So hat beispielsweise der Autozulieferer Continental vor kurzem die Nutzung von WhatsApp auf Diensthandys untersagt. Der Dienstleistungskonzern WISAG und die Deutsche Bank haben die interne Nutzung solcher Apps bereits vor einigen Jahren verboten.

Unternehmen sollten am Arbeitsplatz eine sichere digitale Kommunikation ermöglichen und Datenschutz gewährleisten. Kommunikationsmittel sollten in Kombination mit einem ISO-27001-konformen Managementsystem eingesetzt werden und den Richtlinien der DS-GVO entsprechen. Auch sollte zur zusätzlichen Absicherung mit dem Anbieter der Software ein Vertrag über die Datenverarbeitung unterschrieben werden, worin festgelegt ist, auf welche Daten der Anbieter Zugriff hat und wie diese verwendet und verarbeitet werden.

Darüber hinaus sollte das Tool genauso intuitiv und einfach zu bedienen sein wie die privat genutzten Dienste, damit es von den Mitarbeitern angenommen und der parallele Einsatz von WhatsApp und Co. reduziert wird.

Ein eigens bereitgestelltes Unternehmensnetzwerk (Enterprise Social Network) ist die beste Alternative zu privat genutzten Messenger-Diensten und den sozialen Medien, denn es stellt eine einfach zu bedienende und sichere Kommunikationslösung bereit, die darüber hinaus weitere Vorteile bietet.

Über die Autorin

Lena Bäumges

Customer Success Mangager bei WorkforceIT GmbH

WorkforceIT liefert und implementiert innovative und flexible Mitarbeiter Apps, welche dabei helfen, interne Kommunikation, Onboarding und Personaleinsatzplanung in Unternehmen zu verbessern. Mit Büros in den Niederlanden, Belgien und Deutschland unterstützen wir unsere Kunden, damit sie das Potenzial ihrer Mitarbeiter optimal nutzen können.

▶ www.workforce-it.com/de

DAS BERECHTIGTE INTERESSE ALS RECHTFERTIGUNGSGRUND - EINE PRAXISNAHE DARSTELLUNG

Jutta Oberlin und Dr. Lukas Lezzi

I. Einleitung

Die Datenschutz-Grundverordnung (DS-GVO) bietet den Verantwortlichen die Möglichkeit, eine Datenverarbeitung mit der Verfolgung von eigenen (berechtigten) Interessen (wozu auch Drittinteressen zählen) zu rechtfertigen, sofern diese Interessen diejenigen der betroffenen Personen überwiegen.

Seitdem die damalige Artikel-29-Datenschutzgruppe das berechtigte Interesse als nicht bloss die ultima ratio dargestellt hatte[1], erscheint dieser Rechtfertigungsgrund eine praxisfreundliche und einfache Möglichkeit, eine Datenverarbeitung einer grossen Anzahl von Datensubjekten zu rechtfertigen ohne jeweils eine Einwilligung im Einzelfall einholen zu müssen. Allerdings birgt dieser Rechtfertigungsgrund seine Tücken. Zum einen handelt es bei den berechtigten Interessen um einen unbestimmten und somit auslegungsbedürftigen Rechtsbegriff, welcher von den Aufsichtsbehörden unterschiedlich interpretiert werden kann. Zum anderen sind u.U. zu unterschiedlichen Zeitpunkten zwei Interessenabwägungen durchzuführen, welche auch eine mögliche Quelle zur anderen Beurteilung der Aufsichtsbehörden darstellen.

Nachfolgend soll ein Überblick über diesen Rechtfertigungsgrund der berechtigten Interessen gegeben und anhand von praxisorientierten Beispielen versucht werden diesen Begriff etwas fassbarer zu machen.

II. Grundsatz des Verbots der Datenverarbeitung

Die Art. 6 Abs. 1 DS-GVO bestimmt folgendes: *«Die Verarbeitung ist nur rechtmässig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist…».*

Nach diesem Rechtsprinzip ist etwas grundsätzlich verboten, sofern keine ausdrückliche Erlaubnis vorhanden ist. (Auch das Bundesdatenschutzgesetz (BDSG) in seiner alten Fassung hatte gemäss § 4 Abs. 1 dieses grundlegende datenschutzrechtliche Prinzip eingeführt: *«Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.»)*

Die Rechtmässigkeit der Datenverarbeitung ist sodann mit Ausnahmetatbeständen gemäss Art. 6 Abs. 1 lit. a – f bzw. Art. 9 Abs. 2 lit. a – j DS-GVO abschliessend normiert.

Die Rechtmässigkeit wird jedoch nicht nur durch die Ausnahmetatbestände aus Art. 6 DS-GVO definiert, sondern beinhaltet grundsätzlich auch die Grundsätze aus Art. 5 Abs. 1 DS-GVO.[2]

Dieses Verbot mit Erlaubnisvorbehalt stellt ein sogenanntes Regel-Ausnahme-Prinzip dar, welches zu einer Beweislastumkehr führen kann.

Eine Beweislastumkehr bedeutet im Fall von Datenverarbeitungsvorgängen die Verpflichtung des Verantwortlichen, die rechtmässige Datenverarbeitung bzw. den Rechtfertigungsgrund nachweisen zu können.

Diesbezüglich ist es ratsam, die Rechtsgrundlagen der Datenverarbeitung zu dokumentieren und, wenn es beispielsweise gemäss Art. 6 Abs. 1 lit. f DS-GVO zu Erwägung eines berechtigten Interesses kommt, dieses auch dementsprechend auszulegen und mit dem individuellen Fall zu begründen.

Als kleiner Exkurs ist zu erwähnen, dass das aktuelle Schweizer Datenschutzgesetz ein solches Verbot mit Erlaubnisvorbehalt nicht kennt, sondern den Grundsatz der Erlaubnis einer ▶

[1] Opi–ni–on 06/2014, WP217.

[2] Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung und Intergrität und Vertraulichkeit.

DATENSCHUTZPRAXIS

Datenverarbeitung mit Verbotsvorbehalt aufstellt.[3]

III. Rechtmässigkeit der Verarbeitung von personenbezogenen Daten

Gemäss Art. 5 Abs. 1 lit. a DS-GVO dürfen Daten nur unter gewissen Bedingungen verarbeitet werden: Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz. Dies bedeutet, dass das Kernelement der Norm ein umfassendes präventives Verbot ist, auf welches Ausnahmetatbestände anzuwenden sind.

Die DS-GVO normiert diese Erlaubnistatbestände abschliessend in Art. 6 lit. a - f:

- Einwilligung durch das betroffene Datensubjekt: Auch konkludente Einwilligungserklärungen sind zugelassen[4]
- Verarbeitung betreffend die Erfüllung eines Vertrages
- Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung
- Verarbeitung zum Schutz lebenswichtiger Interessen
- Verarbeitung im Sinne des öffentlichen Interesses
- Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten

Schon bei der Verwirklichung einer dieser sechs Bedingungen ist die Rechtmässigkeit der Datenverarbeitung von personenbezogenen Daten begründet.

Keiner dieser sechs Erlaubnistatbestände wird explizit hervorgehoben und so stehen alle gleichwertig nebeneinander. Auch das oft vermeintlich als nachrangig anzuwendend betitelte berechtigte Interesse aus lit. f sollte weder nach- noch vorrangig angewendet werden.[5]

Das Konzept beinhaltet nicht nur die Gleichstellung aller sechs Elemente, sondern auch die Möglichkeit, dass unter einem Tatbestand mehrere Erlaubnistatbestände verwirklicht werden können. So kann beispielsweise bei der Direktwerbung sowohl das berechtigte Interesse, sowie aber auch die Einwilligung der betroffenen Person in Frage kommen, so denn die betroffene Person ihre Einwilligung erteilt hat.

[3] Vgl. Art. 12 und 13 des schweizerischen Bundesgesetzes über den Datenschutz.

[4] Erwägungsgrund 32.

[5] Artikel 29 Arbeitsgruppe, Stellungnahme 06/2014, 844/14/EN, 13, 62.

[6] Vgl. Frenzel in: Paal/Pauly DSGVO Art. 6 Rn. 9, der einen Zusammenhang zu Art. 5 Abs. 1 lit. c, e DS-GVO herstellt.

[7] Art. 9 DS-GVO.

[8] Vgl. ausführlich Art. 29 Arbeitsgruppe, Stellungnahme 06/2014, 844/14/EN (noch zur DSRL).

Art. 6 Abs. 1 lit. b - f DS-GVO der Norm setzen zudem voraus, dass die Datenverarbeitung für ein gewisses Ziel erforderlich ist.[6] So ist beispielsweise die Verarbeitung von personenbezogenen Daten unter lit. b der Norm zweckmässig um einen Vertrag erfüllen zu können. Beispielsweise ist es bei einem Versicherungsvertrag erforderlich, dass die Versicherung diverse Daten ihres Vertragspartners, wie beispielsweise Name, Adresse, Alter und Nationalität verarbeiten darf.

Eine Spezialregelung findet sich in der Verordnung in Bezug auf die besonderen Kategorien von personenbezogenen Daten.[7] Auch hier besteht ein generelles Verbot mit aufgeführten und abschliessenden Erlaubnistatbeständen. Die Erlaubnistatbestände sind in Art. 9 Abs. 2 lit. a - j DS-GVO normiert.

Die Verarbeitung dieser Daten auf Grundlage der Wahrung des berechtigten Interesses ist nicht möglich.

Eine weitere Spezialregelung findet sich in Art. 49 DS-GVO bzgl. der Datenübermittlungen ins Ausland. Die Zulässigkeit der Datenübermittlungen in Drittländer oder an internationale Organisationen ist mittels eines dreistufigen Systems zu prüfen. Die Stufen stellen sich wie folgt dar:

- Angemessenheitsbeschluss gemäss Art. 45 DS-GVO
- Geeignete Garantien gemäss Art. 46 und 47 DS-GVO
- Ausnahmevorschrift gemäss Art. 49 DS-GVO, wie beispielsweise der in der Praxis bedeutsamste Fall der Einwilligung der betroffenen Person

IV. Die Verarbeitung zur Wahrung berechtigter Interessen gemäss Art. 6 Abs. 1 lit. f DS-GVO

a. Im Allgemeinen

Mit der Auffangklausel in Art. 6 Abs. 1 lit. f DS-GVO ist eine Datenverarbeitung zulässig, wenn diese zur Wahrung eines berechtigten Interesses erforderlich ist.[8]

Unter lit. f können viele verschiedene Sachverhalte subsumiert werden und bewirkt so den Ausgleich zwischen den Interessen der Datensubjekte und denen der Verantwortlichen oder ggf. Dritten.[9]

Lit. f der Norm beinhaltet dabei einen beschränkten persönlichen Anwendungsbereich. Diese Beschränkung entsteht durch Abs. 1 UAbs. 2 DS-GVO mit dem Ausschluss behördlicher Datenverarbeitung.

Grundsätzlich ist beim Erlaubnistatbestand des berechtigten Interesses nicht nur dieses von einem Verantwortlichen erfasst, sondern auch das eines Dritten.

Dabei darf die Auslegung des Sachverhaltes bzw. die Anwendung des berechtigten Interesses nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person verletzen bzw. überwiegen. Besonders bei Kindern ist gemäss lit. f der Norm auf eine besonders enge Auslegung des Rechtsinstitutes des berechtigten Interesses zu achten, da ausdrücklich auf eventuelle überwiegende gegenläufige Belange bei Betroffenheit von Kindern hingewiesen wird.[10]

Der Begriff des berechtigten Interesses ist in der Verordnung nicht weiter definiert. Der Abwägungsvorbehalt, welcher aus lit. f der Norm entsteht, ist sodann zu beachten, wenn es um die Anwendung des berechtigten Interesses als Rechtsgrundlage für eine rechtsmässige Datenverarbeitung geht. Unter dieses kann unter anderem auch das des ideellen oder wirtschaftlichen Interesses eines Verantwortlichen oder Dritten fallen.[11]

Unter den Anwendungsbereich des berechtigten Interesses können sodann folgende Sachverhalte subsumiert werden:

- Gewinnerzielung
- Wissenschaftliche Forschung
- Freie und / oder journalistische Meinungsäusserung
- Verfolgung eigener Rechte[12] (z.B. betriebsinterne Nachforschungen zu Compliance-Fällen)
- Direktwerbung[13]
- Datenaustausch im Konzernsachverhalt[14]
- Verteidigung des eigenen Vermögens, namentlich gegen Betrug und Hackerangriffe[15]
- Datenübermittlung im Zusammenhang mit Straftaten oder Bedrohungen der öffentlichen Sicherheit (auch wenn Verantwortlicher selbst nicht betroffen ist)[16]

In den oben genannten Sachverhalten können die folgenden personenbezogenen Datenkategorien als Bearbeitungsaktivitäten erfasst sein:

- Kundendaten (auch potentielle Kunden, welche Interesse zeigen)
- Mitarbeiterdaten
- Daten von Lieferanten
- Daten von Wettbewerbern

b. Interessenabwägung / Kriterien

Die Verarbeitung im Sinne des berechtigten Interesses muss dazu erforderlich sein, dieses zu schützen und zu wahren.

Ist die Erforderlichkeit gegeben, muss der Verantwortliche evaluieren, ob Interessen der betroffenen Personen der Verarbeitung ihrer personenbezogenen Daten entgegenstehen können. Konkret gibt es hier nur den Richtwert, dass die Auslegung des berechtigten Interesses nicht den Grundfreiheiten und Grundrechten[17] des Datensubjekts zuwiderlaufen dürfen und so die gegenseitigen Belange abzuwägen sind.

So ist ein jeder Ausgangspunkt einer solchen Prüfung die Interessenabwägung zwischen den Persönlichkeitsrechten der betroffenen Person, Auswirkungen auf diese und den Interessen des Verantwortlichen oder Dritten.

Der Konkretisierungsauftrag fällt sodann in Zukunft den Aufsichtsbehörden und den Gerichten, insbesondere dem EuGH, zu.

Bei der Auslegung ist stets auf die Art der Daten der betroffenen Person oder nach der «vernünftigen Erwartung»[18], welche ein Datensubjekt an den jeweiligen individuellen Sachverhalt hat. In der Praxis kann die Erwartung der Datensubjekte mit aufschlussreicher Transparenz des Verantwortlichen beeinflusst werden. So bestätigt die deutsche Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) in ihrem Kurzpapier Nr. 3 die Möglichkeit der Beeinflussung der Interessenabwägung durch den Verantwortlichen:

«Informiert der Verantwortliche transparent und umfassend über eine vorgesehene werbliche Nutzung ▶

[9] Albrecht CR 2016, 88 (92).

[10] Nomos Kommentare, Sydow (Hrsg.), Europäische Datenschutzgrundverordnung: Reimer, S. 350.

[11] Vgl. auch Artikel 29 Datenschutzgruppe, Stellungnahme 06/2014, 844/14/EN, 30 f.

[12] Vgl. EuGH 29.1.2008 – C-275/06, Slg 2008, I-271 – Promusicae: Auskunft über Verbindungsdaten zur Ermöglichung einer Klage.

[13] Erwägungsgrund 47

[14] Erwägungsgrund 48

[15] Erwägungsgrund 49.

[16] Erwägungsgrund 50.

[17] Art. 8 Abs. 1 EUGRCh.

[18] Erwägungsgrund 47 S. 1 Hs. 2.

DATENSCHUTZPRAXIS

der Daten, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Kundendaten entsprechend genutzt werden».[19]

Zu achten ist darauf, dass keine unverhältnismässigen Folgen aus dem Datenverarbeitungsvorgang für das Datensubjekt erwachsen und die Risiken für das Datensubjekt im Vorfeld in die Abwägung mit eingeflossen sind.[20]

Besteht ein Zweifel, ob die konkrete Datenverarbeitung unter das berechtigte Interesse subsumiert werden kann, ist diese nicht von vorneherein einzustellen[21], sondern eher eine Risikoanalyse gemäss Art. 35 DS-GVO mit dem potentiellen Datenverarbeitungsvorgang durchzuführen, welches genaue Risiken und unverhältnismässige Folgen aufzuzeigen vermag. Natürlich muss auch das Risiko vermehrter Widersprüche und gegebenenfalls Sanktionen durch Aufsichtsbehörden in die allgemeinen, betriebsinternen Risikoeinschätzungen des Verantwortlichen miteinbezogen werden.

Auch nach positiver Interessenabwägung zugunsten des berechtigten Interesses des Verantwortlichen oder Dritten ist das Datensubjekt gemäss Art. 21 Abs. 1 DS-GVO jederzeit dazu berechtigt, der Datenverarbeitung zu widersprechen (siehe unten).

c. Prüfung eines Sachverhaltes

Der Verantwortliche ist dazu angehalten einen potentiellen Sachverhalt betreffend des berechtigten Interesses genau zu prüfen und die Interessen aller beteiligter Parteien abzuwägen.

Bei der Interessenabwägung sind sodann auch geeignete Garantien[22] zu berücksichtigen, welche eine positive Auswirkung auf die Evaluierung des berechtigten Interesses haben können. Bei der Prüfung müssen die folgenden Elemente beurteilt und aneinander abgewägt werden:

- Handelt es sich um spezielle Kategorien gemäss Art. 9 DS-GVO? (Keine weitere Prüfung notwendig, da die Wahrung des berechtigten Interesses bei dieser Datenkategorie nicht zulässig ist).
- Ist die Datenverarbeitung erforderlich, um das verfolgte Interesse zu erreichen?
- Handelt es sich bei dem Verantwortlichen bzw. Dritten um eine Behörde? (Die DS-GVO sieht eine Verarbeitungsbefugnis aufgrund der Wahrung des berechtigten Interesses bei Organen und Einrichtungen der Gemeinschaft und von Behörden nicht vor).
- Sind Art, Inhalt und Aussagekraft der betroffenen Daten definiert?
- Ergebnis der Definitionen sind mit dem verfolgten Zweck zu messen. (Aussagekraft der personenbezogenen Daten für den konkret verfolgten Verarbeitungszweck).
- Es ist abzuwägen, ob Daten besonders missbrauchsanfällig sind (beispielsweise Kreditkartendaten).
- Ist aus den Umständen heraus erkennbar, ob die betroffene Person keinen Aussenkontakt wünscht?[23]
- Erfolgt die Datenverarbeitung im Zusammenhang mit einer gewerblichen Tätigkeit der betroffenen Person? (Die Interessen einer gewerblich tätigen natürlichen Person sind zunächst als weniger schutzwürdig einzuordnen, da ohne die Bearbeitung dieser personenbezogenen Daten ein ökonomischer Prozess kaum möglich ist).[24]
- Gibt es unrichtige Daten, welche in die Abwägung einbezogen werden müssen? (Falls ja, müssen diese gemäss Art. 5 Abs. 1 lit. d DS-GVO stets zugunsten der betroffenen Person ausfallen).
- Welche vernünftigen, subjektiven Erwartungen hat das Datensubjekt an die Verarbeitungsaktivitäten?
- Dürfen dies die betroffenen Personen auch objektiv erwarten? (Es kann in einem gewissen Masse auch auf sozial akzeptierte Formen der Datenverarbeitung abgestellt werden).
- Beinhaltet die geplante Datenverarbeitung die Erstellung eines Persönlichkeitsprofils der betroffenen Person? (Wird ein Persönlichkeitsprofil erstellt, ist von einem überwiegenden schutzwürdigen Interesse der betroffenen Person auszugehen).[25]
- Sind angemessene technische und organisatorische Massnahmen bereitgestellt? (Bspw.: Werden Daten verschlüsselt oder pseudonymisiert? Dies kann positiv im Rahmen einer Interessenabwägung berücksichtigt werden).
- Stammen die Daten aus öffentlichen Registern? (Dies kann positiv im Rahmen einer Interessenabwägung berücksichtigt werden).
- Besteht eine vertragliche Absicherung?
- Sind die Betroffenenrechte jederzeit gewährleistet?
- Besteht ein Konzept von beschränkten Zugriffsrechten mit Zugangsprotokoll?
- Werden Daten von Kindern[26] bearbeitet? (Bei Kinderdaten wird gemäss Art. 6 Abs. 1 lit. f DS-GVO von einer überwiegenden Schutzbedürftigkeit der Interessen der betroffenen Person ausgegangen).
- Hat die betroffene Person der Datenverarbeitung gemäss Art. 21 Abs. 1 DS-GVO widersprochen?
- Hat die betroffene Person die Möglichkeit, ihr Widerspruchsrecht gemäss Art. 21 DS-GVO schnell und einfach auszuüben (beispielsweise mittels einer Opt-Out-Option)?
- Hat der Verantwortliche im Falle eines Widerspruchs der betroffenen Person «zwingende schutzwürdige Gründe», um die Datenverarbeitungstätigkeit fortzuführen?
- Findet eine Datenverarbeitung zum Schutz der IT-Sicherheit statt?
- Ist eine Konzerndatenverarbeitung angestrebt? (Gemäss ErwG 48 ist der Datenaustausch innerhalb einer Unternehmensgruppe ausdrücklich als berechtigt anzusehen).
- Wird Direktwerbung betrieben? (siehe dazu detailliert V.)
- Wird ein Retargeting (als Retargeting bezeichnet man eine Technologie im Onlinemarketing, mit der Internetnutzer nach dem Besuch einer Webseite auf anderen Seiten im Netz erneut angesprochen werden[27]) betrieben?
- Werden missbrauchsanfällige Daten wie Standortdaten, Kontodaten usw. verwendet?
- Wurde gemäss Artt. 25 (Privacy by Design) und 35 (Datenschutz-Folgenabschätzung) DS-GVO eine Risikoabschätzung durchgeführt?

d. Rechtsbegriff der vernünftigen Erwartungen

Gemäss Erwägungsgrund 47 sind die vernünftigen Erwartungen der betroffenen Person in der Abwägungsprüfung einzubeziehen. Die vernünftige Erwartung bezieht sich in diesem Zusammenhang auf das Verhältnis, welches die betroffene Person mit dem Verantwortlichen hat. Hier ist zudem auf eine etwaige Rechtsbeziehung, Geschäftstätigkeit, Datenkategorien usw. abzustellen.

Auch ein Blick in die Zukunft bedarf es bei dieser Art von Evaluation. Der Verantwortliche muss im Vorfeld einschätzen, ob die betroffene Person vernünftigerweise abschätzen kann, ob möglicherweise eine Verarbeitung für die vom Verantwortlichen geplanten Zwecke erfolgen kann.[28]

Auf der einen Seite sind die subjektiven Erwartungen der betroffenen Personen zu berücksichtigen.[29] Hier stellt sich jedoch die Frage, wie genau der Verantwortliche diese Erwartungshaltungen im Vorfeld feststellen oder gar berücksichtigen sollte. Aus dem Wort «vernünftigerweise» im Erwägungsgrund 47 lässt sich aber schliessen, dass auch ein objektiver Massstab an die Erwartungshaltungen gelegt werden darf. Die subjektive Erwartung wird dementsprechend bei der vorstehend dargelegten Interessenabwägung kaum in Betracht fallen. Vielmehr kann sich der Verantwortliche auf die objektivierte Erwartungshaltung, insbesondere auf sozial akzeptiere Arten der Datenverarbeitung, abstützen.

In den Informationen, die den betroffenen Personen aufgrund von Artt. 13 und 14 DS-GVO zu Verfügung gestellt werden müssen, können durch eine weitgehende Transparenz durchaus auch Erwartungshaltungen begründet werden. Allerdings findet diese Möglichkeit ihre Grenze an dem objektiven Massstab, was vernünftigerweise in der konkreten Situation erwartet werden darf.[30]

Ist es der betroffenen Person nicht möglich, auf vernünftige Weise eine solche zukünftige Datenverarbeitung abzuschätzen, ist davon auszugehen, dass die Interessen der berechtigten Person, dass eine Datenverarbeitung nicht stattfindet, in diesem Falle überwiegen.

e. Konsquenzen

i. Informationspflicht

Falls wie oben dargelegt, der Verantwortliche den Rechtsfertigungsgrund des berechtigten Interesses für eine Datenverarbeitung beansprucht, so löst dies eine in Art. 21 Abs. 4 DS-GVO nomierte ▸

[19] DSK – Datenschutzkonferenz: Kurzpapier Nr. 3 Verarbeitung personenbezogener Daten für Werbung, 29.06.2017.

[20] Artikel 29 Datenschutzgruppe, Stellungnahme 06/2014, 844/14/EN, 52.

[21] EuGH 13.5.2014 – C-131/12.

[22] Beispielsweise Pseudonymisierung, Verschlüsselung, die Möglichkeit der raschen Wiederherstellung der Verfügbarkeit von personenbezogenen Daten bei einem Zwischenfall, Risiko Assessments, vertragliche Absicherungen usw.

[23] Weichert in DKWW BDSG Paragraph 29 Rn. 16.

[24] Vgl. OLG Stuttgart Urt. V. 12.12.2002 – 2 U 103/02, NJW-RR 2003, 1410 (1412).

[25] Gola/Schomerus BDSG Paragraph 29 Rn. 18.

[26] Als Kind ist gemäss UN Kinderrechtskonvention (Art. 1 der Konvention über die Rechte des Kindes v. 20.11.1989) und aus der Definition in den Entwürfen und des Parlaments (Art. 4 Nr. 18 DSGVO-E), jede Person zu subsumieren, welche das achtzehnte Lebensjahr noch nicht vollendet hat.

[27] http://www.digitalwiki.de/retargeting/.

[28] Erwägungsgrund 47.

[29] Orientierungshilfe der (deutschen) Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) vom November 2018, 4.

[30] Orientierungshilfe der (deutschen) Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) vom November 2018, 4.e.

Anzeige

Informationspflicht des Verantwortlichen aus. Gemäss dieser Vorschrift muss die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation mit ihr ausdrücklich auf das Widerrufsrecht hingewiesen werden; Dieser Hinweis hat in einer verständlichen und von anderen Informationen getrennten Form zu erfolgen. Diese Informationspflicht stellt aber keine lex specialis gegenüber den allgemeinen Anforderungen an eine Information in Artt. 13 und 14 DS-GVO dar, sondern ist jeweils im Zusammenhang mit diesen Artikeln zu verstehen.[31]

Grundsätzlich muss immer ein Hinweis erfolgen, wenn eine Datenverarbeitung auf berechtigtem Interesse beruht. Das Widerspruchsrecht ist der betroffenen Person gemäss Art. 21 Abs. 4 DS-GVO zum Zeitpunkt der ersten Kommunikation mitzuteilen. Weil aber im Bereich der Datenverarbeitungen aufgrund berechtigten Interesses eine vorgängige Kommunikation mit den betroffenen Personen nicht stattfindet, kommen die allgemeinen Zeitpunkte der Information gemäss Artt. 13 und 14 DS-GVO zur Anwendung. Das heisst, dass bei Direkterhebung im Zeitpunkt der Erhebung und bei Erhebung von personenbezogenen Daten bei Dritten spätestens nach einem Monat über das Widerspruchsrecht informiert werden muss.[32]

Art. 21 Abs. 4 DSVGO legt weiter fest, dass die Information ausdrücklich, verständlich und in getrennter Form von übrigen Informationen zu ergehen hat. Diese Anforderungen sind dahingehend zu verstehen, dass die Information über das Widerspruchsrecht in einer Weise hervorzuheben ist, dass sie klar von anderen Informationen zu unterscheiden ist und auch von Personen ohne Fachwissen sofort verstanden werden kann. Beispielsweise kann dies durch optische Hervorhebung, wie etwa eine gesonderte Textbox, und gleichzeitiger typografischen Auszeichnung, wie etwa Schriftstil, erreicht werden. In inhaltlicher Hinsicht ist die Information so abzufassen, dass klar ersichtlich ist, gegen welche Datenverarbeitung man Widerspruch einlegen kann und wo ein solcher Einspruch angebracht werden kann. Eine Einbindung dieser Information in die Datenschutzerklärung ist also grundsätzlich möglich, sofern das Widerspruchsrecht klar vom Rest getrennt ist. Denkbar wäre am Anfang oder Ende einer solchen Kommunikation eine hervorgehobene Textbox anzubringen und in dieser auch gleich die entsprechende Kontaktadresse anzugeben.

[31] Herbst in: Kühling/Buchner DS-GVO, Art. 21 N 34.

[32] Kramer in: Auernhammer DGVO/BDSG, Art. 21 N 33.

[33] Herbst (Fn. 22), Art. 21 N 15.

[34] Kramer (Fn. 23), Art. 21 N 10.

[35] Kamann/Braun in: Ehmann/Selmayr Datenschutz-Grundverordnung, Art. 21 N 23.

ii. Widerspruchsrecht

Wie oben bereits ausgeführt haben die betroffenen Personen grundsätzlich einen Anspruch darauf, dass der Verantwortliche eine Datenverarbeitung ihrer personenbezogenen Daten, die auf berechtigten Interessen beruht, einstellt. Hierbei wird zwischen dem absoluten und dem relativen Widerspruchsrecht unterschieden.

Das absolute Widerspruchsrecht kommt gemäss Art. 21 Abs. 2 DS-GVO ausschliesslich bei Datenverarbeitungen zu Direktwerbung, einschliesslich Profiling, zur Anwendung. In diesem Fall muss die betroffene Person ihren Widerspruch nicht begründen, sondern nur gegenüber dem Verantwortlichen kommunizieren. Der Verantwortliche muss daraufhin die Verarbeitung zu Direktwerbezwecken gegenüber dieser Peson einstellen.

Anders ist es dagegen beim sogenannten relativen Widerspruchsrecht. Hier muss gemäss Art. 21 Abs. 1 DS-GVO die betroffene Person nachdem sie den Widerspruch angemeldet hat, Gründe darlegen, die sich aus ihrer besonderen Situation ergeben und einer weiteren Datenverarbeitung entgegenstehen. Es wird sich insbesondere um Gründe handeln müssen, die vom Verantwortlichen in der allgemeinen Interessensabwägung nicht bekannt sein und dementsprechend auch nicht berücksichtigt werden konnten.[33] Beispielshaft können die folgenden Gründe aufgezählt werde: besondere familiäre oder geschäftliche Situationen, besondere Stellung in der Öffentlichkeit, Gefahr für Leib und Leben oder vorgefallene Datenschutzverletzungen durch den Verantwortlichen.[34]

Falls ein solches relatives Widerspruchsrecht geltend gemacht wird, muss der Verantwortliche gemäss Art. 21 Abs. 1 DS-GVO zwingende Gründe für eine Weiterverarbeitung nachweisen, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder die Verarbeitung dient für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Solche zwingenden Gründe können insbesondere in der Betrugsbekämpfung oder der Wahrung der Datensicherheit erkannt werden.[35]

Falls keine zwingenden Gründe für eine Weiterverarbeitung vorliegen, welche die geltend gemachten Interessen überwiegen, so muss der Verantwortliche die Verarbeitung in konkreten Fall einstellen.

V. Ausgewählte Anwendungsfälle

a. Marketingaktivitäten und das berechtigte Interesse

Wie dargelegt, kommt der Direktwerbung als absoluter Widerspruchsgrund eine grosse Bedeutung innerhalb der DS-GVO zu. Der Begriff selbst wird aber in der Verordnung nicht definiert. Als mögliche Definition kann der Begriff der Werbung, wie er in Art. 2 lit. a der Richtlinie 2006/114/EG definiert ist, herangezogen werden. Demnach ist Werbung jede Äusserung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern.[36] Aber auch Umfragen, Anfragen zur Bewertung von erbrachten Dienstleistungen oder gekauften Produkten oder etwa auch Anschreiben von politischen Parteien oder wohltätigen Organisationen lassen sich als Werbung qualifizieren.[37]

Als Rechtsgrundlage für Direktwerbung kommt neben den Einwilligungen insbesondere das berechtigte Interesse in Frage. Andere Rechtfertigungsgründe sind aber grundsätzlich auch denkbar, jedoch in der Praxis kaum vertreten. Die Interessensabwägung hat, wie oben dargelegt, auch im Bereich der Direktwerbung in Bezug auf den konkreten Einzelfall stattzufinden und die Interessen, Recht und Freiheiten, aber auch subjektiven Erwartungshaltungen der betroffenen Personen, zu berücksichtigen.

Bei der Beurteilung aller Umstände relevant sind insbesondere die Art der Datenerhebung bzw. die Herkunft der Daten sowie der beabsichtigte Kommunikationsweg. So kann die allgemeine Aussage gemacht werden, dass je invasiver ein Kommunikationsweg (z.B. ein Telefonanruf gegenüber einer E-Mail) oder je weiter die Quelle der Daten von den betroffenen Personen entfernt ist (z.B. indirekte Erhebung gegenüber der direkten Erhebung), desto weniger wird ein Verantwortlicher auf seine Interessen zur Datenverarbeitungn berufen können.[38]

In der Praxis besonders bedeutsam ist die Bestandskundenwerbung. Hier besteht grundsätzlich ein berechtigtes Interesse, Werbung zu versenden. Allerdings darf dies nicht schematisch angewandt werden, sondern es ist etwa auch zu berücksichtigen, ob es sich um eine Privat- oder Geschäftskundenbeziehung handelt oder auch wie lange der letzte Kontakt zurückliegt.[39]

Beispielsweise sehr problematische ist die Verwendung «alter Datenbestände», welche sich über die Jahre aus verschiedenen Marketinginitiativen bzw. verschiedenen Verarbeitungsvorgängen im Bereich Marketing angesammelt haben. Diese Art von Datenbeständen sind noch viel zu oft in Marketingabteilungen von Unternehmen vorzufinden und führen beispielsweise alleine schon aufgrund der fehlenden Transparenz bzw. Nachvollziehbarkeit[40] und der fehlenden Information an die betroffene Person[41], zur Nicht-Konformität mit der DS-GVO.

[36] Art. 2 Ziff. 1 Richtlinie irreführende und vergleichende Werbung; EuGH GRUR Int 2002, 50, 52 – Toshiba.

[37] Siehe dazu Orientierungshilfe der (deutschen) Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) vom November 2018, 3.

[38] Siehe dazu Orientierungshilfe der (deutschen) Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) vom November 2018, 4 ff. und 10 ff.

[39] Orientierungshilfe der (deutschen) Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) vom November 2018, 6.

[40] Art. 5 Abs. 1 lit. a DS-GVO.

[41] Art. 13 und 14 DS-GVO.

DATENSCHUTZPRAXIS

b. Online-Tracking

Im Bereich des Online-Tracking vertreten die deutschen Aufsichtsbehörden eine strenge Auffassung, welche eine Datenverarbeitung mit Tracking-Massnahmen und Nutzerprofilen aufgrund des berechtigten Interesses nicht mehr möglich macht. Dieser zufolge muss im Vorfeld eine Einwilligung der betroffenen Person eingeholt werden.[42]

Kulanz gegenüber der Auslegung im Sinne des berechtigten Interesses lässt die deutsche Litertur zu.[43]

Sie lässt beim Online-Tracking ein Profiling gestützt auf das berechtigte Interesse zu, verlangt dabei aber, dass das Profiling pseudonymisiert bzw. verschlüsselt erfolgt, d.h. dass Nutzerprofile nicht mit eindeutigen Identifikatoren der betreffenden Nutzer zusammengeführt werden.

VI. Praktische Vorgehensweise zur Einhaltung der Compliance

Nachfolgend sind einige Punkte aufzuführen, die für die Einhaltung der Compliance im Bereich der Datenverarbeitung aufgrund berechtigter Interessen von Bedeutung sind.

- Genaue Inventarisierung aller Datenverarbeitungstätigkeiten, um Datenverarbeitungen zu erkennen, welche auf berechtigten Interesssen beruhen.
- Erstellen eines Prozesses zur Durchführung und Dokumentation der Interessenabwägung, insbesondere sollte hier der Datenschutzbeauftragte involviert werden, sofern vorhanden.
- Evaluation der Folgen für das betroffene Datensubjekt.
- Es muss sichergestellt werden, dass mit der Verfolgung der berechtigten Interessen die Rechte und Freiheiten der betroffenen Personen nicht ernsthaft beeinträchtigt werden.
- Belange betroffener Kinder sind besonders gewichtig zu beachten.
- Prüfung, ob eine Zweckänderung gemäss Art. 6 Abs. 4 DS-GVO vorliegt.
- Erstellen der speziellen Information an die betroffenen Personen über das Widerspruchsrecht.
- Erstellen eines Prozesses zur Interessenabwägung bei Geltendmachung des relativen Widerspruchsrechts mit klaren Kriterien.
- Erstellen eines Prozesses zur Sicherstellung, dass bei stattgegebenem Widerspruch die Datenverarbeitung eingestellt wird.
- Der Datenschutzbeauftragte ist jeweils beizuziehen.

VII. Schlussbetrachtung

Der Rechtfertigungsgrund der berechtigten Interessen ist ein zweischneidiges Schwert. Auf der einen Seite gibt es den Verantwortlichen die Möglichkeit, in ihren Datenverarbeitungen flexibel zu bleiben und eigene Interessen zu verfolgen, ohne jeweils eine Einwilligung einholen zu müssen. Auf der anderen Seite besteht immer noch eine grosse Rechtsunsicherheit in Bezug auf den unbestimmten Rechtsbegriff «berechtigtes Interesse». Hier braucht es noch Leitlinien des Europäischen Datenschutzausschusses oder der Aufsichtsbehörden, damit eine einheitliche Auslegung und Anwendung dieses Rechtfertigungsgrundes angestrebt werden kann.

Bis dahin besteht für Verantwortliche, die sich auf berechtigte Interessen berufen, das Risiko, dass eine Aufsichtsbehörde die Interessen anders beurteilt und dies zu Sanktionen führt.

Für die Veranwortlichen ist es deshalb entscheidend, dass sie die geforderte Güterabwägung für das berechtigte Interesse unter Einbezug des Datenschutzbeauftragten nach klaren Kriterien durchführen und gemäss Art. 5 Abs. 2 DS-GVO sauber dokumentieren. Zudem ist über die Datenverarbeitung transparent zu informieren und insbesondere das Widerspruchsrecht klar hervorzuben.

Weiter sind Prozesse einzuführen, damit Widersprüche von betroffenen Personen zuverlässig registriert, gegebenfalls eine Interessenabwägung im Einzelfall vorgenommen und die Ergebnisse sauber dokumentiert werden können. Schliesslich ist sicherzustellen, dass bei stattgebenden Widersprüchen die Weiterverarbeitung per sofort eingestellt wird und unter Umständen die Daten gemäss Art. 17 DS-GVO unwiderruflich gelöscht werden.

Mit einer sauberen Dokumentation und funktionierenden Prozessen, insbesondere zur Einstellung von Datenverarbeitungen, lässt sich aber sagen, dass es wohl nicht ein zu grosses Risiko ist, sich zum jetzigen Zeitpunkt auf das berechtigte Interesse zu berufen.

Über die Autoren

Jutta Sonja Oberlin

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

Dr.iur. Lukas Lezzi, CIPP/E

hat in Zürich Rechtswissenschaften studiert und im Finanzmarktrecht promoviert. Er war als betrieblicher Datenschutzverantwortlicher einer grossen schweizerischen Finanzmarktinfrastruktur tätig. Zurzeit bereitet er sich auf die Zürcher Anwaltsprüfung vor. Er ist insbesondere im Bereich des schweizerischen Datenschutzrechts und der DS-GVO tätig.

Anzeige

[42] Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Nr. 9.

[43] SCHWARTMANN/KLEIN: Heidelberger Kommentar der DSGVO/BDSG, RN. 138 ff.

DATENSCHUTZPRAXIS – ADVERTORIAL

UNTERSCHÄTZTE HERAUSFORDERUNG: DIE NACHWEISPFLICHTEN NACH ARTT. 5 UND 24 DS-GVO ENTWICKELN SICH ZUM KNACKPUNKT DER UMSETZUNG

Interview mit Christian Volkmer

Christian Volkmer,
Projekt 29 GmbH & Co. KG

Seit fast einem Jahr ist die europäische Datenschutz-Grundverordnung (DS-GVO) inzwischen scharf gestellt. Langsam wird deutlich, wo die größten Lücken in der Umsetzung klaffen. „Die Musik spielt bei der Accountability, also den vielfältigen Verpflichtungen die korrekte Umsetzung der DS-GVO nachzuweisen“, sagt Christian Volkmer, geschäftsführender Gesellschafter des Regensburger Datenschutz-Spezialisten Projekt 29. „Viele Audits, auch bei Risikoträgern wie Banken oder Medizindienstleistern, offenbaren hier große Lücken.

Nach Art. 5 Abs. 1 DS-GVO muss der Verantwortliche nicht nur dafür sorgen, dass die Prinzipien der DS-GVO eingehalten werden, sondern er muss nach Abs. 2 die Einhaltung auch nachweisen. In der englischen Fassung der Verordnung taucht hier der Begriff „Accountability“ auf. Das lässt sich mit Rechenschaftspflicht ins Deutsche übersetzen. Die Nachweispflicht findet sich dann in Art. 24 Abs. 1, der besagt, dass der Verantwortliche den Nachweis dafür erbringen können muss, „dass die Verarbeitung gemäß dieser Verordnung erfolgt“.

„Viele Vorschriften der DS-GVO zum konkreten Schutz personenbezogener Daten hatten sich ja in ähnlicher Form auch schon im Bundesdatenschutzgesetz gefunden. Die Rechenschafts- und Nachweispflichten aber sind komplett neu“, so Volkmer. Und der Experte erläutert die Tragweite an einem einfachen Beispiel, dem Recht auf Löschung nach Art. 17.

Bisher, sagt Volkmer, sei dem Gesetz genüge getan gewesen, wenn auf Verlangen des Betroffenen die Daten tatsächlich gelöscht wurden. Nach DS-GVO folgen aus Art. 17 aber vier Dokumentationspflichten.

Erstens muss der Prozess als solcher definiert und beschrieben werden: Was müssen die Mitarbeiter tun, wenn eine Kunde die Löschung seiner Daten verlangt.

Zweitens muss der Datenverarbeiter nachweisen können, dass die Mitarbeiter tatsächlich wissen, was sie tun müssen. Nötig ist der Nachweis eine Schulung, eine schriftliche Handlungsanweisung oder ein ähnliches Dokument.

Drittens muss die konkrete Umsetzung dokumentiert werden: Wann und wie ging die Bitte um Löschung ein, wann und wie wurde sie umgesetzt.

Viertens muss dokumentiert sein, dass der Prozess Löschersuchen in regelmäßigen Abständen überprüft wird und welche Ergebnisse die Überprüfung gezeigt hat.

„Stellt sich bei der Prüfung heraus, dass beim Löschen alles klappt und wird das dokumentiert, dann ist alles gut“, sagt Volkmer. „Wenn nicht, dann gilt es nachzujustieren. Und zu dokumentieren: Welche Fehler sind aufgefallen, wie wurde der Prozess geändert, wie wurden die Mitarbeiter geschult und so weiter.“

Datenschutz als dynamischer Prozess

Das Datenschutzhandbuch, in dem einmal für alle Zeiten steht, wie mit personenbezogenen Daten umgegangen wird, reicht also nicht aus. „Das erfüllt höchstens ein Drittel des insgesamt geforderten Umfangs“, so Volkmer. Die Dokumentation muss ständig fortgeschrieben und ergänzt werden, denn Datenschutzmanagement nach DS-GVO bedeutet einen dynamischen Prozess. Wie im Qualitätsmanagement nach ISO 9001 oder im Informationssicherheits-Management nach ISO 27001 gefordert, muss auch das Datenschutzmanagement zyklisch nach der PDCA-Methode aktualisiert werden. „P“ steht für das englische „plan“, also planen. Dieser Schritt entspricht noch am ehesten dem gewohnten Verfahrensverzeichnis. Als Verfahren wird aufgeschrieben, was unter bestimmten Umständen passieren muss. „D“ steht für „do“, also die konkrete Umsetzung des Verfahrens. „C“ meint „check“, die Überprüfung, ob das Verfahren tatsächlich in allen Fällen korrekt umgesetzt worden ist. Fällt dabei auf, dass doch nicht alles korrekt läuft, gilt „A“ oder „act“: Der im ersten Schritt gefasste Plan, das Verfahren, muss korrigiert werden.

DATENSCHUTZPRAXIS – ADVERTORIAL

Rechenschaftspflicht bedeutet Nachweislast-Umkehr

Die Brisanz des Themas Rechenschaftspflicht lässt sich aus den Aktivitäten der Landes-Datenschutzbehörden ableiten. Im Herbst 2018 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) zwei Prüfverfahren zum Stand der Umsetzung der DS-GVO aufgesetzt (siehe: www.lda.bayern.de/de/kontrollen). Eines untersucht kleine und mittelständische Unternehmen ab 100 Mitarbeitern. „Der dreiseitige Fragebogen hat es in sich", sagt Volkmer. 20 Themengebiete fragt die Aufsichtsbehörde ab und verlangt zu fast jedem Einzelnen davon, die Dokumentation vorzulegen. Im erläuternden Text auf seiner Website weist das BayLDA ausdrücklich darauf hin: „Die DS-GVO verlangt vom Verantwortlichen, dass die Einhaltung der DS-GVO nachgewiesen wird (Art. 5 Abs. 2 DS-GVO). Diese ‚Rechenschaftspflicht' stellt vom Grundsatz her eine ‚Nachweislast-Umkehr' dar, was bedeutet, dass die Einhaltung der gesetzlichen Anforderungen der Aufsichtsbehörde bei einer Kontrolle dargestellt werden muss."

Aus Sicht von Projekt 29 ergibt sich die Accountability nach DS-GVO für 20 verschiedene Themenbereiche, einige mit höherer, andere mit geringerer Priorität. Für wichtig hält Christian Volkmer unter anderem folgende Punkte.

Erteilung der Einwilligung, Art. 7 DS-GVO

Einwilligungen zur Datenverarbeitung müssen nicht nur eingeholt werden, es muss auch dokumentiert werden, dass sie für jeden einzelnen Fall vorliegen.

Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte des Betroffenen, Art. 12 DS-GVO

In einem Register muss hinterlegt sein, wo überall Erklärungen zum Umgang mit personenbezogenen Daten veröffentlicht sind. Das können Websites, Infoflyer, Verträge, der Onlineshop und andere Stellen mehr sein. Ändert sich etwas in der Datenschutzerklärung, muss die Organisation wissen, wo überall sie das anzupassen hat.

Datenschutz durch Technik, Art. 25 DS-GVO

Hierbei geht es um die technischen und organisatorischen Maßnahmen (TOM), die im Verarbeitungsverzeichnis aufgeführt sein müssen. Neu ist, dass in einer Risikobewertung abgeschätzt werden muss, ob die ergriffenen TOM dem Risiko eines Datenabflusses angemessen sind – was wiederum dokumentiert sein muss.

Umsetzung der Speicherbegrenzung, Art. 5 DS-GVO

Ist dokumentiert, welche Daten im Unternehmen vorliegen, wo sie abgespeichert sind, wann sie im Einzelnen gelöscht werden müssen? Zum Löschkonzept hat das BayLDA mit dem Thema Archive und Backups eine weitere kniffelige Frage in seinen Erhebungsbogen aufgenommen. Denn ein Unternehmen muss sicherstellen und dokumentieren, dass gelöschte Daten nicht über den Umweg eines zurückgespielten Backups wieder zum Leben auferstehen.

Umsetzung der Sicherheit der Verarbeitung, Art. 32 DS-GVO

„Platz 1 der IT-Sicherheitsbedrohungen stellen heute Computersysteme dar, die nicht regelmäßig upgedatet werden", weiß Christian Volkmer. Das Management von Sicherheitsupdates, die Schulung der Mitarbeiter und die regelmäßige Überprüfung und Nachjustierung der Maßnahmen müssen dokumentiert werden.

Umgang mit Datenschutzverletzungen, Art. 33 DS-GVO

Nach dem alten deutschen Recht lag eine Datenschutzverletzung vor, wenn tatsächlich Daten abgeflossen waren. Die DS-GVO betrachtet es schon als Verstoß, wenn nicht auszuschließen ist, dass Daten abgeflossen sein könnten. Jeder Verdachtsfall muss dokumentiert werden. „Mitarbeiter müssen sich also eventuell selbst kleinerer Schlampereien zum Beispiel auf der Dienstreise bezichtigen. Das Thema ist sensibel. Damit sie das tun, brauchen sie ein hohes Bewusstsein, wie wichtig Datenschutz und das Datenschutzmanagement inzwischen sind", sagt Volkmer.

Darstellung der Meldepflicht an Aufsichtsbehörden, Art. 33 DS-GVO

Das BayLDA fragt: „Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?" Dazu bedarf es eines definierten Prozesses, der geschult und regelmäßig überprüft werden muss – samt seiner Dokumentation.

Dokumentation von Audits

Dabei reichte früher die Bestätigung, dass ein Audit stattgefunden hat. Heute will die Behörde es laut ihrem Fragebogen genauer dokumentiert haben: „Sind … die letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?"

„Wer sich intensiv mit dem Thema beschäftigt sieht schnell ein: Mit Worddokumenten oder Excel-Files kann weder das Management nach dem PDCA-Zyklus noch die Dokumentation so gelingen, dass die Behörde bei einer Prüfung zufrieden wäre", gibt sich Volkmer überzeugt. Sein Unternehmen hat deswegen Privacysoft entwickelt, eine Online-Software, die Verantwortliche an die Hand nimmt und Schritt für Schritt durchs Datenschutzmanagement leitet. Nach den ersten Erfahrungen mit den neuen Rechenschafts- und Nachweispflichten legt Projekt 29 einen besonderen Schwerpunkt auf das entsprechend Modul in Privacysoft. „Wir haben es so weiterentwickelt, dass Verantwortliche genau wissen, was zu tun ist", sagt Volkmer. Und den Fragebogen des BayLDA nicht mehr fürchten müssen.

Über 20 Jahre Erfahrung bei Datenschutz und IT-Sicherheit

Schon seit den 1990er Jahren beschäftigt sich Christian Volkmer mit IT-Sicherheit. Bei einem der weltgrößten Softwarehersteller war er für Datenschutz und Sicherheit der deutschen Rechenzentren verantwortlich. 1996 gründete er sein erstes Beratungsunternehmen, aus dem die Projekt 29 Gruppe hervorging. Die Mitarbeiter der Gruppe halten heute über 3.800 Mandate als externe Datenschutzbeauftragte. Das Unternehmen betreut Verbände, Vereine, Arztpraxen und Kammern sowie Firmen aller Branchen von 10 bis 56.000 Mitarbeitern.

Projekt 29 GmbH & Co. KG
Ostengasse 14
93047 Regensburg
Telefon 0941 2986930
info@projekt29.de

▶ www.projekt29.de
▶ www.privacysoft.de

Christian Volkmer,
geschäftsführender Inhaber
der Projekt 29 Gruppe

AUFSICHTSBEHÖRDE

„DATENSCHUTZBEAUFTRAGTE BEDEUTEN KEINEN BÜROKRATIEAUFWAND“

Interview mit BfDI Ulrich Kelber

Seit seinem Amtsantritt Ende Januar setzt sich der neue Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Ulrich Kelber, für den Datenschutz ein. Die BvD-News sprach mit ihm über seine Kritik an Facebook und WhatsApp, über die Abstimmungen der europäischen Datenschutzbehörden und die künftige Rolle der Datenschutzbeauftragten in Deutschland.

© Fotos: Susie Knoll

BvD-News: Herr Kelber, wie schätzen Sie das Verhältnis der Deutschen zum Thema Datenschutz ein? Sind sie zu uninteressiert?

Ulrich Kelber: Im Gegenteil. Die Sensibilität hat eindeutig zugenommen. Das sieht man an einer Reihe von Verhaltensänderungen. Die Bereitschaft zum Beispiel Mobilfunknummern oder persönliche Fotos frei zu geben, ist sehr zurückgegangen. Wir brauchen aber weiter mehr Aufklärung, damit die Verbraucher wissen, wie sie sich und ihre Daten schützen können.

BvD-News: Sie äußerten bereits Kritik an Facebook und WhatsApp. Das Bundeskartellamt hat mittlerweile die Verbindung von Daten beider Dienste zur Profilerstellung untersagt. Verbraucher und Unternehmen, selbst manche Behörden, halten die Dienste aber für unverzichtbar. Was sagen Sie denen?

Ulrich Kelber: Dass ich sie grundsätzlich verstehen kann. Allerdings sollte ebenfalls jedem klar sein, dass sich auch Facebook und WhatsApp an Recht und Gesetz halten müssen. Wenn dies passiert, spricht auch nichts gegen ihre Nutzung. Bis dahin ist es unsere Aufgabe Druck aufzubauen, um das europäisches Datenschutzrecht durch zusetzen. Im Fall von Facebook sind die irischen Kollegen als zuständige Datenschutzbehörde jetzt aufgerufen, Entscheidungen zu den eingegangenen Beschwerden zu treffen und diese dann mit den anderen Datenschutzbehörden abzustimmen. Sollten wir mit diesen nicht einverstanden sein, werden wir als deutsche Aufsichtsbehörden die neuen Möglichkeiten des europäischen Datenschutzrechts, also Kohärenzverfahren, bis hin zu einer Abstimmung im europäischen Datenschutzausschusses nutzen, um die Rechte der Bürgerinnen und Bürger zu schützen.

BvD-News: Wie können Sie Druck aufbauen, zum Beispiel, um „Privacy by Design“ bei den Social-Media-Giganten durchzusetzen?

Ulrich Kelber: Spezifisch bei Privacy by Design oder Privacy by Default werden wir zunächst definieren müssen, was das ganz konkret heißt und anbieten, Unternehmen bei der Umsetzung der Vorgaben zu unterstützen. Sollte dies nicht fruchten und an Stellen, wo es erforderlich ist, die Vorgaben nicht eingehalten werden, haben wir aufgrund der DS-GVO Möglichkeiten, das geltende Recht durchzusetzen.

BvD-News: Die Instrumente, die die Datenschutz-Grundverordnung dafür bereithält, reichen Ihrer Einschätzung nach aus? Oder sehen Sie Nachbesserungsbedarf?

Ulrich Kelber: Wir haben auf jeden Fall erst mal Instrumente in der DS-GVO, die dafür sorgen, dass man sich nicht hinter nationalen Regeln verstecken kann. Wir müssen uns natürlich jetzt anschauen, wie die in der Praxis funktionieren.

BvD-News: Welche Rolle kommt den Verbrauchern dabei zu? Wie können sie Druck auf die Konzerne aufbauen?

Ulrich Kelber: Ich glaube, dass das gar nicht so aufwendig ist. Wenn ich vorerst nicht auf den Dienst verzichten will oder kann, von dem ich gelesen habe, dass er mit dem Schutz meiner Daten und jener von Freunden, Familie und Arbeitskollegen nicht gut umgeht, dann sollte ich zumindest eine Alternative dort einsetzen, wo es mir möglich ist. Auf den heutigen Smartphones können durchaus zwei oder mehrere Messenger-Dienste gleichzeitig genutzt werden. Dann kann man zum Beispiel die Familiengruppe schon auf einen Messenger-Dienst umstellen, der in puncto Datenschutz wesentlich unproblematischer ist.

BvD-News: Auch manche Pläne der Bundesregierung sehen Sie kritisch, etwa jene, alle Fahrzeuge vor Diesel-Fahrverbotszonen zu erfassen oder die flächendeckende Gesichtserkennung einzuführen. Welche Chancen sehen Sie, solche Entwicklungen mit einem fairen Datenschutz auszustatten oder gar zu stoppen?

Ulrich Kelber: Wir können keine Gesetze stoppen. Allerdings beraten wir den Gesetzgeber beim Gesetzgebungsverfahren und weisen in diesem Zusammenhang auch explizit auf datenschutzrechtliche Probleme hin. Im Idealfall werden wir dann auch gehört und der entsprechende Entwurf angepasst. Untersagen können wir lediglich konkrete Handlungen mit Datenschutzbezug, wenn diese ohne eine rechtliche Grundlage erfolgen. Das ist das Durchsetzungsrecht der Aufsichtsbehörde.

BvD-News: Sie hatten sich selbst für mehr Transparenz bei Bußgeldverfahren und -entscheidungen ausgesprochen und dazu im eigenen Hause ein Konzept angeregt. Wann können wir mit dessen Umsetzung rechnen?

Ulrich Kelber: Ich lasse derzeit prüfen, ob wir Informationen, die im Rahmen des Informationsfreiheitsgesetzte abgefragt werden können, nicht auch aktiv zur Verfügung stellen sollten. Das würde grundsätzlich auch Kontrollberichte betreffen. Ich hoffe, dass wir ein solches Transparenzverfahren bis zum Ende des Frühjahrs entwickeln können.

BvD-News: Bei der Einführung der Datenschutz-Grundverordnung hagelte es viel Kritik. Wo sehen Sie Reformbedarf?

Ulrich Kelber: Derzeit sind wir noch in der Umsetzungsphase. Viel Potenzial haben wir noch gar nicht ausgeschöpft. Aber in der Tat haben wir den Auftrag erhalten, zusammenzufassen, wo wir Lücken sehen. Beispielsweise kann ich mir gut vorstellen, dass die Bereiche Profiling und Scoring klarer geregelt werden. Auch werden wir uns damit auseinandersetzen, ob wir nicht die Informations- und Dokumentationspflichten speziell für kleine und mittelständische Unternehmen erleichtern können.

BvD-News: Es gibt in einigen Bundesländern und auch beim Bundesinnenministerium Bestrebungen, die Benennungspflicht von Datenschutzbeauftragten gerade für kleine und mittlere Unternehmen zu lockern. Wie schätzen Sie diese Diskussion ein?

Ulrich Kelber: Zu allererst: Datenschutzbeauftragte bedeuten keinen Bürokratieaufwand. Der Datenschutzbeauftragte hilft dem Unternehmen, die Pflichten, wahrzunehmen, die ihm die DS-GVO auferlegt. Die Idee, die Voraussetzungen für die Benennung eines Datenschutzbeauftragten schlechter zu regeln als vor der DS-GVO würde am Ende den Unternehmen schaden, die von der Benennung befreit wären. Denn sie wären damit ja nicht vom Datenschutz befreit. Sinnvoller wäre es zu überlegen, etwa die Informations- und Dokumentationspflichten zu erleichtern, vor allem im unmittelbaren Kundenkontakt. Darüber kann man in diesem und nächstem Jahr unaufgeregt sprechen. Aber bitte nicht den rein symbolischen oder am Ende fehlerhaften Schritt machen, die Berufung von Datenschutzbeauftragten hinter das alte Schutzniveau abzusenken.

BvD-News: Was kommt denn generell auf die Datenschutzbeauftragten zu? Wie sehen Sie künftig in deren Rolle und Funktion?

Ulrich Kelber: Der Datenschutzbeauftragte wird zunehmend und mehr als in der Vergangenheit eine koordinierende und beratende Funktion bekommen. Den Unternehmen muss klar werden, dass die Datenschutzkonzepte nicht in erster Linie von Datenschutzbeauftragten entwickelt, sondern von ihm überprüft und kontrolliert werden. Ansonsten wäre das eine Selbstkontrolle. Ich glaube, es ist gut, mit dem Datenschutzbeauftragten jemanden zu haben, der sich übergreifend im Unternehmen Gedanken zu dem Thema macht und nicht in der Fachlichkeit eines Betriebs und seiner Abläufe gefangen ist.

Anzeige

29

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.

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

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

Datenschutzdokumentation | Vorlagen und Checklisten | Vorgangsmanagement | Online-Schulungen | Mehrsprachig

INNOVATIONSPREIS-IT BEST OF 2018 initiative mittelstand IT-SECURITY

Software Bundesverband IT-Mittelstand Made in Germany 100% Service Qualität Zukunft

Software Hosted in Germany Bundesverband IT-Mittelstand e.V.

bevh PREFERRED BUSINESS PARTNER

BvD e.V. MITGLIED DATENSCHUTZ GESTALTEN

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

WEBSITES IM DATENSCHUTZCHECK AM SID 2019:

WAS WEBSITEBETREIBER WISSEN SOLLTEN, UM DATENSCHUTZVERSTÖSSE ZU VERMEIDEN

Alexander Buckel

Zusammenfassung

Während das Jahr 2018 insbesondere von der immensen Beratungstätigkeit der Aufsichtsbehörden rund um die Datenschutz-Grundverordnung (DS-GVO) geprägt war, zeichnet sich bereits im Frühjahr diesen Jahres ab, dass Verantwortliche nun verstärkt mit Datenschutzkontrollen durch die zuständigen Aufsichtsbehörden rechnen müssen. Die erste umfangreiche Prüfung aus 2019 des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA) fand am Safer Internet Day (SID) statt und offenbarte bei den geprüften Websites zum Teil gravierende Mängel. Im BayLDA stellt sich mittlerweile nicht mehr die Frage, ob es bei solchen Verstößen zur Bußgeldverfahren kommt, sondern nur noch wann.

Verstärkte Prüfungen durch das BayLDA

Tausende Datenschutzbeschwerden seit DS-GVO-Anwendbarkeit

Spätestens der neue Tätigkeitsbericht des BayLDA für die Jahre 2017/2018 wird auch dem letzten Zweifler klar machen, dass die Anzahl der eingehenden Fälle mit der dazugehörigen Arbeitslast einen neuen Rekordhöhepunkt in der Datenschutzaufsichtsbehörde erreicht hat. Die Ursache dafür ist schnell ausfindig gemacht: die DS-GVO. Rund um den Mai vergangenen Jahres haben sich aus verständlichen Gründen bei Verantwortlichen und Datenschutzbeauftragten tausende von Datenschutzfragen rund um die neue Verordnung ergeben. Das BayLDA hatte ein großes Interesse daran, durch gezielte Beratungen – sei es persönlich vor Ort oder durch Vorträge auf Veranstaltungen – die vielen Unklarheiten und zum Teil auch die kursierenden Falschmeldungen zur DS-GVO abzubauen. Nun, ein dreiviertel Jahr später, ist ein solcher Beratungsaufwand durch das BayLDA in der aktuellen Personalausstattung nicht mehr zu leisten, da die Anzahl der eingehenden Datenschutzbeschwerden förmlich „explodiert" ist. Auch die Meldungen von Unternehmen über Datenschutzverletzungen nehmen überhand und haben sich fast verzwanzigfacht im Vergleich zu den vorherigen Jahren – Prognose: weiter steigend.

Mehr Datenschutzkontrollen von Websites

Diese Entwicklungen führen dazu, dass das BayLDA die eigenen Kapazitäten noch stärker auf seine gesetzlichen Pflichtaufgaben wie die Beschwerdebearbeitung bündeln muss. Viele der eingereichten Datenschutzbeschwerden handeln von potentiellen Verstößen auf Websites. Meist geht es darin um die Themen Information, Einwilligung, Cookies und Tracking. Gleichzeitig zeigen die tausenden Datenpannenmeldungen nach Art. 33 DS-GVO, dass zahlreiche Schwachstellen bei Websites oft einem sicheren Betrieb und Umgang mit Nutzerdaten im Weg stehen: Immer wieder werden durchaus gravierende Hacking-Fälle bei der Behörde eingereicht, die im Vorfeld durch geeignete Maßnahmen des Websitebetreibers hätten vermieden werden können.

Safer Internet Day als Prüfrahmen

Unter dem Motto „*Together for a better internet*" bot der Safer Internet Day 2019 vielen Institutionen die Möglichkeit, auch dieses Jahr einen Beitrag für ein sicheres Internet zu leisten. Mit dem Wissen über die zuvor genannten bestehenden Problemfelder im Web hat sich das BayLDA vorgenommen, in Form zweier Datenschutzchecks zur Cybersicherheit und zum Tracking am SID 2019 teilzunehmen und feststellen, ob ausgewählte Websites die Anforderungen der DS-GVO zum Schutz der Nutzerdaten ausreichend umsetzen. Die vom BayLDA initiierte Prüfaktion sollte ihren Anteil für ein sicheres Internet beitragen und gleichzeitig dafür sorgen, dass einige der in den Beschwerden vorgetragenen Sachverhalte durch die Behörde offiziell kontrolliert werden. Zudem sollten die Ankündigung der Prüfung und die beabsichtigte transparente Veröffentlichung der Prüfergebnisse alle Websitebetreiber hinsichtlich datenschutzrechtlicher Anforderungen sensibilisieren. ▸

Datenschutzkontrollen am SID 2019: Zahlreiche Websites im Fokus

Auswahl der Unternehmen und Prüfpunkte zur Cybersicherheit

Die Sicherheit eines Nutzerkontos und der Schutz der digitalen Identität des Nutzers hängen maßgeblich von zwei Faktoren ab: Dem Nutzer selbst und dem Websitebetreiber. Es handelt sich um ein Zusammenspiel, bei dem beide Parteien ihren Anteil zur Sicherheit leisten müssen. Der für den jeweiligen Dienst verantwortliche Betreiber trägt dabei aber eine ganz besondere Rolle, da der Nutzer ihm seine persönlichen Informationen und das eigene Passwort anvertraut. Aus diesem Grund hatte sich das BayLDA entschlossen, sich näher anzusehen, wie gerade die Websitebetreiber den Nutzer durch den Registrierungs- und Login-Prozess begleiten und mit den Passwörtern ihrer Nutzer umgehen. Im Rahmen des mehrstufigen Sicherheitschecks wurden verschiedene Punkte in unterschiedlicher Tiefe untersucht.

Für diesen Prüfblock wurden vom BayLDA äußerst prominente Websites ausgewählt: Entweder haben diese eine vorragende Platzierung im Ranking der meistbesuchten Websites in Deutschland oder gehören zu den umsatzstärksten deutschen Online-Plattformen (eCommerce). Somit sollte gewährleistet werden, dass mit den untersuchten Websites auch eine sehr große Reichweite hinsichtlich deutscher Online-Nutzer erreicht wird. In der Summe wurden 20 Websites hinsichtlich des sicheren Umgangs mit Nutzerdaten, insbesondere der Passwörter, geprüft: Neben bekannten Sozialen Netzwerken und Videostreaming-Portalen wurden auch verschiedene Online-Shops, E-Mail-Dienste und digitale Foto-Services untersucht.

Nachfolgend findet sich eine Auswahl der Fragen und Punkte, die bei diesen Websites näher betrachtet wurden:

Cybersicherheitscheck - Block I	Registrierung - Sichere Gestaltung eines Nutzer-Accounts
HTTPS	*Verfügt der Dienst über eine ausreichende HTTPS-Verschlüsselung zum Schutz der eingegebenen personenbezogenen Daten?*
Nutzerkennung	*Wird die E-Mail-Adresse als verpflichtendes Login-Element verwendet oder kann bei der Registrierung auch ein Pseudonym frei gewählt werden?*
Info zur Passwortwahl	*Wird der Nutzer unterrichtet, wie ein sicheres (starkes) Passwort gewählt werden kann?*
Mindestlänge Passwort	*Wie lang ist die Mindestlänge des Passworts?*
Wahl eines starken Passworts	*Wird ein starkes Passwort vom System „erzwungen"?*
Anzeige der Passwortstärke	*Wird dem Nutzer die Stärke seines gewählten Passworts angezeigt?*
2-Faktor	*Wird dem Nutzer auch eine Zwei-Faktor-Authentifizierung an?*
Info zum zweiten Faktor	*Werden dem Nutzer der Mehrwert und die Durchführung einer Zwei-Faktor-Authentifizierung verständlich erläutert?*
Sicherheits-E-Mail-Adresse und Mobilfunknummer	*Kann der Nutzer zur Sicherheit eine zweite E-Mail-Adresse oder eine Mobilfunknummer hinterlegen?*
Info zur Sicherheits-E-Mail-Adresse und Mobilfunknummer	*Wird dem Nutzer erklärt, wann über die zweite E-Mail-Adresse bzw. die Mobilfunknummer eine Benachrichtigung erfolgt?*
Bestätigung der zweiten E-Mail-Adresse/Mobilfunknummer	*Muss die hinterlegte zweite E-Mail-Adresse bzw. die Mobilfunknummer bestätigt werden (z. B. SMS-Code)?*
Sicherheit der Nutzerangaben	*Werden persönliche Informationen aus der Registrierung in der URL als Parameter mit übertragen?*
Dritte	*Werden persönliche Informationen aus der Registrierung an Dritte (z. B. Tracking-Anbieter) übertragen?*
Bestätigung der Registrierung	*Erhält der Nutzer eine E-Mail zur Registrierung, um den Account zu bestätigen (evtl. mit URL-Token)?*
Account-Daten per E-Mail	*Werden persönliche Daten aus der Registrierung dem Nutzer per E-Mail zugesandt?*
Information zu Phishing	*Wird der Nutzer bei oder kurz nach der Registrierung über Gefahren möglicher Phishing-Angriffe informiert?*

Cybersicherheitscheck - Block II	Login - Schutz vor Übernahme des Nutzer-Accounts durch Hacker
Fehlversuche / Brute Force	*Wird der Login nach einer Anzahl von mehreren Fehlversuchen gesperrt oder verzögert (Online-Passwortattacke, Schutz vor Brute Force)?*
Login aus der Fremde	*Ist ein Login mit einer IP-Adresse aus für den Nutzer untypischen Ländern möglich?*
Fehlgeschlagene Logins	*Wird der Nutzer nach erfolgreichem Login darüber informiert, ob es fehlgeschlagene Logins gab und was dies zu bedeuten hat?*
Info über offene Sitzungen	*Kann der Nutzer in der Weboberfläche aktive (offene) Sitzungen erkennen und diese auch beenden?*
Passwortänderung: Abfrage Passwort	*Wird bei Passwortänderung das bestehende (alte) Passwort erneut abgefragt?*
Info zur Passwortänderung an Mobilfunknummer/Mail-Adresse	*Wird der Nutzer bei einer Passwortänderung an seine E-Mail-Adresse, seine Zweit-E-Mail-Adresse oder Mobilfunknummer informiert?*
Passwort-Vergessen-Angaben	*Werden bei der Passwort-Vergessen-Funktion Fragen zu den Account-Angaben gestellt?*
Passwort-Vergessen-Verfahren	*Erfolgt das Passwort-Zurücksetzen über eine zeitlich begrenzt gültige URL, die an die hinterlegte E-Mail-Adresse gesendet wird?*
Support bei Hacking	*Wird dem Nutzer auf der Website des Dienstes leicht und verständlich Hilfe angeboten, wenn der eigene Account gehackt wurde?*

Datenschutzcheck „Tracking" (Information & Einwilligung)

Im anschließenden Teil „Tracking" wurden dagegen ausschließlich bayerische Unternehmen bzw. deren Websites für diese Datenschutzkontrolle bestimmt. Hier befanden sich auf Grund konkret vorliegender Beschwerden von Bürgern bereits 40 Websites auf der Prüfliste, wobei alle diese Websites ausschließlich von großen bzw. sehr großen bayerischen Firmen betrieben und verantwortet werden.

Im Rahmen dieses Checks wurden zahlreiche Fragen aus dem Bereich der Information und Einwilligung zum Thema Tracking abgehandelt. Folgende wesentliche Fragestellungen gehörten dazu:

- Sind auf der Website Tracking-Tools eingebunden, die umfangreiche Profile der Nutzer anlegen?
- Wird der Nutzer vorab transparent über den Einsatz von Tracking-Tools informiert?
- Fordert die Website über einen „Cookie-Banner" die Einwilligung des Nutzers für das praktizierte Tracking?
- Werden die Anforderungen an eine wirksame Einwilligung von der Website erfüllt?
- Kann der Nutzer die Profilbildung durch Tracking-Tools auf der Website selbst durch eigene Einstellungen im Browser verhindern?

▸

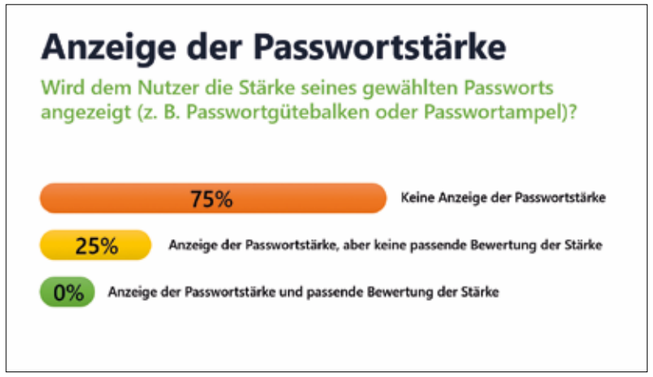
AUFSICHTSBEHÖRDE

Ergebnis der SID-Prüfung: Überraschend viele Mängel bei Websites

Sicherheit bei Websites noch ausbaufähig

Obwohl das BayLDA im Cybersicherheitscheck sehr große Websites hinsichtlich längst bekannter Sicherheitsanforderungen untersuchte, musste festgestellt werden, dass zahlreiche Defizite vorhanden waren. In einer umfassenden Ergebnispräsentation stellt das BayLDA die einzelnen Ergebnisse auf seiner Website zur Verfügung, bewertet diese und informiert über den Hintergrund des jeweiligen Prüfpunktes.

Nachfolgend ist ein Auszug zu den durchaus überraschenden Erkenntnissen aufgeführt: Ein starkes Passwort ist eigentlich die entscheidende Komponente, um die persönlichen Informationen in einem Nutzer-Account vor Fremden zu schützen. Daher ist es wichtig, dass der Nutzer vom Anbieter Hinweise erhält, wie er selbst ein starkes Passwort erzeugen und so seine eigenen Daten schützen kann. Durch die Prüfung wurde klar, dass ein Großteil der Websites dem Nutzer bei der Passwortwahl nur unzureichende Hinweise mit an die Hand gibt. In manchen dieser Fälle wird der Nutzer überhaupt nicht unterrichtet, wie sich ein starkes Passwort zusammensetzen soll – der Nutzer ist somit völlig auf sich allein gestellt. In drei Viertel der Fälle gibt es keinerlei Anzeige der Passwortstärke.



Gleichzeitig besitzen viele Dienste aber eine zu geringe Mindestlänge bei der Wahl von Passwörtern (z. B. vier oder sechs Zeichen) – dies genügt nicht, um ein starkes Passwort zu erhalten. In der Untersuchung wurde dabei festgestellt, dass keiner der Online-Dienste ein starkes Passwort „erzwingt". Der einzige Dienst aus dem Prüflauf, der eine Mindestlänge von zehn Zeichen anbietet, fordert keine ausreichende Komplexität, so dass auch dort schwa-

che Passwörter möglich sind. Negativ fällt auf, dass einige Passwortrichtlinien nicht zeitgemäß sind und einfache, unsichere Passwörter nach bekanntem Muster gewählt werden können. Noch viel erschreckender ist jedoch die Tatsache, dass einige Websites diese offensichtlich schwachen Passwörter als sicher bewerten. Im Test wurden Passwörter wie „0000", „123456" oder auch „Passwort" von manchen Diensten zugelassen.

Tracking unter der DS-GVO bleibt Reizthema

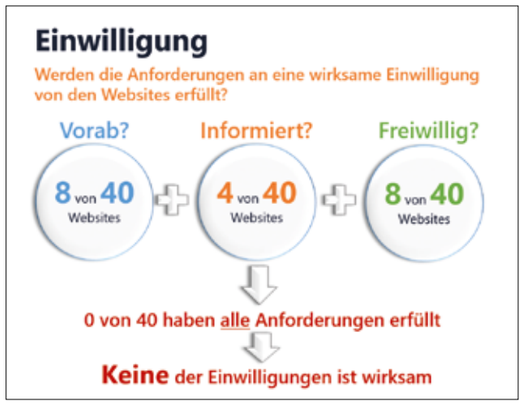
Im Datenschutzcheck „Tracking" war das Ergebnis desolat: Keine der geprüften Websites erfüllte die Anforderung an eine zulässige Einwilligung nach der DS-GVO, obwohl alle geprüften Websites Tracking-Tools von Drittanbietern einbinden und somit eine Datenverarbeitung durch fremde Dienste veranlassen. Besucht ein Nutzer einer dieser Website, so werden automatisch Daten des Nutzers im Hintergrund an Drittanbieter gesendet.

Viele Website-Betreiber verschweigen den Einsatz von Tracking-Tools; andere hingegen informieren pauschal über verschiedenste Tools, die zum Teil gar nicht auf der Website eingebunden sind. Im Ergebnis wird der Nutzer nur selten transparent darüber informiert, ob und welche seiner Daten für welche Zwecke verarbeitet werden.

Von den geprüften Websites setzen 30 sogenannte „Cookie-Banner" ein. Über ein solches Cookie-Banner soll der Nutzer eine Einwilligung für die Verarbeitung seiner Daten abgeben. Die Prüfung ergab, dass alle Einwilligungen, die über Cookie-Banner eingeholt wurden, unwirksam sind. Eine Einwilligung ist nur wirksam, wenn sie vorab erteilt wird, d. h. wenn alle Tracking-Skripte blockiert sind, solange bis der Nutzer aktiv zugestimmt hat. Außerdem muss die Einwilligung freiwillig sein und der Nutzer vorab über die Datenverarbeitung informiert werden. Ist auch nur eine dieser Voraussetzungen nicht berücksichtigt, so ist die Einwilligung rechtswidrig. Im Gesamtergebnis konnte bei keiner der 40 geprüften Websites eine wirksam eingeholte Einwilligung festgestellt werden. Es bleibt daher auch in den nächsten Monaten spannend, ob und wie sich die Aufsichtsbehörden gemeinsam bezüglich der Datenschutzanforderungen hinsichtlich Tracking positionieren und diese dann auch konsequent vollziehen. Das BayLDA weist in seiner Pressemitteilung vom 5. Februar 2019 bereits darauf hin, die Einleitung von Bußgeldverfahren zu prüfen.

Ausblick auf weitere Online-Kontrollen

Die durchgeführte Datenschutzprüfung des BayLDA am SID 2019 wird sicherlich nicht die letzte Großprüfung gewesen sein. Gerade im Umfeld von Online-Diensten ist mit verstärkten Kontrollen zu rechnen, da mittlerweile selbst kleinere Unternehmen vermehrt ihre Dienstleistungen in Form von Webauftritten anpreisen. Verantwortliche und Datenschutzbeauftragte sollten sich hierbei bewusst machen, dass Datenschutzverstöße auf Websites für Nutzer, aber auch für Aufsichtsbehörden sehr leicht festzustellen und zu protokollieren sind. Websitebetreiber sollten sich daher mit den bekannten Anforderungen vertraut machen und geeignete Maßnahmen ergreifen. Viele der für Websites erforderlichen Datenschutzpunkte sind tatsächlich mit wenig Aufwand und so-



mit auch überschaubaren Kosten realisierbar. Diese positive Randnotiz dürfte manchen Verantwortlichen dazu bewegen, sich eher zeitnah und aktiv der Sache anzunehmen als darauf zu hoffen nie „erwischt" zu werden. Letztendlich muss festgehalten werden, dass es sich bei einigen der in der Prüfung festgestellten Mängel grundsätzlich um bußgeldbewehrte Verstöße handelt. Sollte es zu Bußgeldern kommen, ist davon auszugehen, dass diese bei weitem die Kosten der erforderlichen Maßnahmen übersteigen.

Weiterführende Links:

- Pressemitteilung des BayLDA zur Prüfankündigung am SID (1. Februar 2019)
  ▶ www.lda.bayern.de/media/pm2019_2.pdf
- Pressemitteilung des BayLDA zu den Ergebnissen der Prüfung am SID (5. Februar 2019)
  ▶ www.lda.bayern.de/media/pm2019_3_de.pdf
- Ergebnispräsentation der Prüfung am SID (5. Februar 2019)
  ▶ www.lda.bayern.de/media/sid_ergebnis_2019.pdf
- Pressemitteilung des BayLDA zur Buchveröffentlichung für Websitebetreiber (12. Oktober 2018)
  ▶ www.lda.bayern.de/media/pm2018_15.pdf

Über den Autor

Alexander Buckel

ist Wirtschaftsinformatiker und stellvertretender Leiter des Referats für Cybersicherheit und technischen Datenschutz im Bayerischen Landesamt für Datenschutzaufsicht. Seit 2011 ist er Teil der Aufsichtsbehörde und führt in seinem Aufgabenbereich regelmäßig technische Datenschutzprüfungen bayerischer Verantwortlicher rund um das Thema „Sicherheit von Webdiensten" durch. Kernstücke seiner Arbeit sind daher auch gezielte Präventionsmaßnahmen für Websitebetreiber gegen Angriffe über das Internet sowie Incident-Response-Pläne bei Datenschutzverletzungen.

Seit dem Herbst 2018 ist der Ratgeber „DS-GVO und ePrivacy-VO auf Websites umsetzen – 250 praktische Antworten plus kompakte Checklisten von Datenschutzexperten" verfügbar, bei dem Alexander Buckel als einer von drei Autoren wesentlich mitgewirkt hat. In leicht verständlichen Schritten werden darin die neuen datenschutzrechtlichen Anforderungen für Websites mit dem Ziel dargestellt, Verstöße bereits im Vorfeld durch einfache Maßnahmen proaktiv zu vermeiden und somit das eigene Bußgeldrisiko zu reduzieren.

AUFSICHTSBEHÖRDE

SCHULSTUNDEN DER ETWAS ANDEREN ART ODER: DATENSCHÜTZER EROBERN DIE SCHULEN ODER: DATENSCHÜTZER UND SCHÜLER LEHREN UND LERNEN GEMEINSAM

Safer Internet Day 2019

Quelle Photo: erschienen in der Rhein-Neckar-Zeitung vom 6. Februar 2019, Photographin: Helmut Pfeifer

Schulstunden der etwas anderen Art wurden im Februar 2019 durch die Mitarbeiterinnen und Mitarbeiter der Datenschutz-Aufsichtsbehörden in verschiedenen Bundesländern angeboten.

Es handelt sich hierbei nicht um ein redaktionelles Versehen - tatsächlich wurden im Rahmen einer gemeinsamen länderübergreifenden Aktion und in Kooperation mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. Schülerinnen und Schüler mit dem Themengebiet Datenschutz vertraut gemacht.

Doch alles der Reihe nach:

Im November des letzten Jahres hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, zu einem Round Table nach Stuttgart eingeladen. Mit am Tisch saßen Vertreter von Aufsichtsbehörden verschiedener anderer Bundesländer und auch Vertreter der Initiative „Datenschutz geht zur Schule“ des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Ziel dieser Einladung und dieses Round Tables war es, die bereits bestehende Initiative des BvD „Datenschutz geht zur Schule“ zu unterstützen und weiter auszubauen.

Die BvD-Initiative „Datenschutz geht zur Schule“ wurde im Jahr 2009 gegründet und hat sich die Sensibilisierung von Kindern und Jugendlichen im Umgang mit personenbezogenen Daten im Internet auf die Fahne geschrieben.

Mit Anwendbarkeit der Europäischen Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 besteht mit Artikel 57 Absatz 1 lit. b DS-GVO ein gesetzlicher Auftrag, dem sich alle Datenschutzaufsichtsbehörden in ganz Europa stellen müssen.

Damit wird die Verpflichtung zum Schutz der Rechte von Kindern erstmalig in einer europaweit geltenden Rechtsgrundlage für Datenschutz explizit festgeschrieben.

Unabhängig von dieser gesetzlichen Forderung und diesem Novum in der Rechtslandschaft, kann der Schutz von Kindern und Jugendlichen gar nicht hoch genug angesiedelt werden, handelt es sich doch um die Schutzbedürftigsten in unserer Gesellschaft. Datenschutz bedeutet nicht nur Schutz der persönlichen Freiheit, sondern insbesondere auch Kinder- und Jugendschutz, so der Landesbeauftragte für Datenschutz von Baden-Württemberg, Dr. Stefan Brink. Als Vater von drei Kindern ist ihm der Kinder- und Jugendschutz ein großes Anliegen. Besonderes Augenmerk legt er dabei darauf, nicht zu verbieten, sondern die Kinder und Jugendlichen stark zu machen, damit sie Risiken erkennen und so in die Lage versetzt werden, **bewusst** zu agieren und **bewusst** und gut informiert zu entscheiden.

Brink warb bei den Vertretern der anderen Bundesländer, um deren Engagement und Unterstützung.

Schnell waren sich alle Beteiligten des baden-württembergischen Round Tables darüber einig die Initiative „Datenschutz geht zur Schule“ des BvD zu unterstützen und eine gemeinsame länderübergreifende Aktion an einem möglichst prominenten Termin durchführen zu wollen.

Welcher Termin könnte sich dafür besser eignen als der Safer Internet Day?

Der Safer Internet Day wird jedes Jahr am zweiten Tag der zweiten Woche des zweiten Monats durch die EU-Initiative klicksafe organisiert.

Dr. Stefan Brink, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, koordiniert auf Seiten der Aufsichtsbehörden das Projekt. „Kinder und Jugendliche wachsen mit den digitalen Angeboten auf. Dadurch sind sie aber einem besonderen Risiko ausgesetzt“, sagte er. „Deshalb ist es uns ein Anliegen, insbesondere junge Menschen für das Thema Datenschutz zu sensibilisieren. Wir freuen uns dies in einer bundeslandübergreifenden Kooperation der Aufsichtsbehörden gemeinsam mit dem BvD umzusetzen.“

Brink weiter, „mit den teilnehmenden Aufsichtsbehörden sind wir von Niedersachsen bis Bayern prima aufgestellt.“

Allein in seinem Haus meldeten sich mehr als zehn Mitarbeiterinnen und Mitarbeiter für die ungewöhnlichen Unterrichtseinheiten. „Das zeigt ein hohes Maß an persönlichem Engagement unserer Fachleute für den Datenschutz“, unterstrich er.

Pünktlich zum Safer Internet Day bekam die Initiative „Datenschutz geht zur Schule“ des BvD damit tatkräftige Unterstützung von den Aufsichtsbehörden in Baden-Württemberg, Bayern, Niedersachen und Rheinland-Pfalz.

„Die Kooperation mit den vier Aufsichtsbehörden hilft uns, viel mehr Heranwachsende beim Thema Datenschutz zu erreichen“, sagte der Sprecher der BvD-Initiative, Rudi Kramer. „Denn sicher im Netz zu surfen ist eine Grundvoraussetzung für junge Menschen, selbständig und bewusst eigene Entscheidungen online treffen zu können.“

Bei ihrem Unterricht greifen die Mitarbeiter der Aufsichtsbehörden auf das BvD-Material von „Datenschutz geht zur Schule“ zurück, dessen Weiterentwicklung inhaltlich von der EU-Initiative klicksafe und finanziell von der DATEV-Stiftung Zukunft unterstützt wurde.

Besonders kurzweilig und vor allem anschaulich wird das doch recht abstrakte Thema „Datenschutz“ durch die zahlreichen im Vortrag enthaltenen kurzen Videoclips transportiert.

Bemerkenswert waren auch die Diskussionen um Big Data. Das abstrakte Thema wurde mit einem Videoclip eingeführt, bei dem der Kunde eines Pizzalieferdienstes im Rahmen seiner Pizza-Bestellung mit einigen überraschenden privaten Informationen konfrontiert wird. Wußte doch der Mitarbeiter des Lieferdienstes nach Blick in das persönliche Profil des Kunden, u. a. dass der hungrige Kunde an Übergewicht leide und zu hohe Cholesterinwerte aufweise. Sollte er dennoch eine Pizza bestellen wollen, müssten im Pizzapreis diese Risikofaktoren mit einem Zuschlag veranschlagt werden. Der sichtlich irritierte Kunde mochte diesen völlig überhöhten Pizzapreis nun mit seiner Kreditkarte begleichen, was der Pizzadienstmitarbeiter mit dem Hinweis auf einen Flug, den der Kunde in der Vergangenheit nicht beglichen hätte, ablehnte und auf Barzahlung bei Lieferung bestand.

Bei der anschließenden Diskussion wurden das Für und Wieder dieser „Allwissenheit“ ausgiebig durch die Schülerinnen und Schüler mit den Vertretern der Aufsichtsbehörden erörtert. Einige Schüler vertraten die Meinung, dass ein ▸

allwissender Pizzadienst doch sehr bequem wäre, während andere Schüler dies wohl praktisch, aber doch auch gruselig fanden.

Wer will denn schon, dass der Fremde am anderen Ende der Telefonleitung bei der Pizzabestellung weiß, wer welche gesundheitlichen Probleme hat oder welche Rechnungen noch nicht bezahlt wurden….?

Auch wurde im Rahmen der facettenreichen Diskussionen deutlich, dass viele einzelne Informationen erst durch die maschinelle Auswertung und Zusammenführung Rückschlüsse auf viele andere Gebiete, wie bspw. Interessen, Geschlecht, sexuelle Orientierung,…. möglich werden.

Schnell war der Kern der Thematik erreicht und die Schüler hinterfragten bspw. die Grenzen von Big Data, Smart Home und auch die Nutzung und Datenweitergabe beim Einsatz von Messengerdiensten, um den Preis der Preisgabe von privaten Informationen und Daten.

Bequemlichkeit versus Privatsphäre wurde schnell zu einem großen Thema.

Es wurde deutlich, dass kostenfreie Angebote kritisch zu hinterfragen sind. Ist ein kostenlos angebotener Messengerdienst tatsächlich kostenlos? Aus welchem Grund bieten viele Unternehmen Kundenkarten und damit verbunden Rabatte und Treueprämien an? Schnell wurde klar, dass in der heutigen Zeit kein Unternehmen etwas zu verschenken hat.

Wie finanzieren sich also diese Rabattaktionen, diese kostenlosen Messengerdienste und welchen Nutzen hat ein gewinnorientiertes Unternehmen von solchen Angeboten und Maßnahmen?

Diese Frage ließ sich nicht auf Anhieb durch die Schülerinnen und Schüler beantworten. Erst eine genauere gemeinsame Betrachtung mit den Dozentinnen und Dozenten der Aufsichtsbehörden brachte zum Vorschein, dass kostenlos offensichtlich nur so zu verstehen ist, dass kein Geld im eigentlichen Sinn fließt. Für die Schülerinnen und Schüler wurde daraufhin schnell klar, dass bspw. die Messengerdienste auf die in ihrem Handy gespeicherten Adressdaten zugreifen können, dass ersichtlich ist, mit wem sie sich treffen, wie oft sie sich treffen, welche Interessen sie haben,….

Und, dass auch die Unternehmen, die Kundenkarten anbieten, ganz detailliert darüber informiert sind, was und wieviel eingekauft wird, ob Bedarf an Alkohol oder Babywindeln besteht,…..Aufgrund dieser Informationen lassen sich z. B. Rückschlüsse auf die Anzahl der Personen in diesem Haushalt ziehen und, und, und.

Überraschend deutlich wurde für die Dozentinnen und Dozenten aus den Aufsichtsbehörden, dass die „Datenkrake“ Facebook nahezu keine Bedeutung in dieser Altersklasse hat – Facebook nutzen nur die Erwachsenen, also die Eltern oder die Großeltern. Und wer will schon eine Freundschaftsanfrage seiner Tante – so das Feedback der Schülerinnen und Schüler.

Die begeisterten Rückmeldung von Schülerinnen und Schülern, Lehrerinnen und Lehrern, Schulleiterinnen und Schulleitern, Dozentinnen und Dozenten der jeweiligen Aufsichtsbehörden und auch das Presseecho in den regionalen Tageszeitungen haben deutlich gemacht, wie wichtig und sinnvoll es ist Kinder und Jugendliche im Umgang mit ihren personenbezogenen Daten im Internet zu sensibilisieren und welche Herausforderung es auch darstellt dieses Thema mit einem zielgruppengerechten Wortschatz zu erläutern.

Konkret wurden in Bad Friedrichshall, Borsdorf, Esslingen, Ettlingen, Glemsaue, Göttingen, Hannover, Helmstedt, Hohenheim, Hermannsburg, Herrenberg, Hildesheim, Hille, Koblenz, Lauterecken, Lippstadt, Lorch, Ludwigsburg, Lüneburg, Mainz, Neuendettelsau, Osnabrück, Pforzheim, Regensburg, Sarstedt, Springe, Stuttgart, Trossingen, Walldorf, Waltrop, und Winnweiler insgesamt rund. 2.700 Schüler und Schülerinnen mit der gemeinsamen und länderübergreifenden Aktion der Aufsichtsbehörden in Kooperation mit dem BvD erreicht.

Deutlich wurde jedoch auch, dass der Bedarf an den Schulen viel, viel höher ist, als wir mit unserer Aktion befriedigen konnten.

Fazit unserer länderübergreifenden Aktion:

Wir werden weitermachen!

Machen Sie mit!

Werden Sie auch Dozent bei der Initiative „Datenschutz geht zur Schule“.

An der Initiative „Datenschutz geht zur Schule“ können sich alle Datenschützer beteiligen, die eine Qualifizierungsmaßnahme für die Sensibilisierung von Schulklassen durchlaufen haben.

Weitere Informationen finden Sie unter:

▶ https://www.bvdnet.de/datenschutz-geht-zur-schule/

Für Lehrkräfte, die selbst Aspekte des Datenschutzes im Unterricht behandeln oder die Einheiten vor- und nachbereiten wollen, liegt seit November 2018 die 3. neu überarbeitete Auflage des Lehrerhandbuchs „Datenschutz geht zur Schule“ vor. Die Materialien können kostenlos unter www.bvdnet.de/datenschutz-geht-zur-schule heruntergeladen werden.

Über die Autorin

Martina Strifler
Datenschutz als KULTuraufgabe

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg

▶ www.baden-wuerttemberg.datenschutz.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

Anzeige

Wichtiges Datenschutzwissen für Ihre Kollegen

Mitarbeiterinformation zum Datenschutz

BvD-Rabatt 30%

TKMmedia

Kommen Sie Ihrer Verpflichtung zum Datenschutz nach und schulen Sie Ihre Mitarbeiter mit der kompakten Infobroschüre. Jetzt auch in englischer Sprache!

Profitieren Sie von unseren BVD-Staffelpreisen:

→ Einzelpreis für BVD-Mitglieder	6,98 €/Stk.
→ 10-50 Stk. für BVD-Mitglieder	4,87 €/Stk.
→ 51-100 Stk. für BVD-Mitglieder	4,13 €/Stk.
→ 101-500 Stk. für BVD-Mitglieder	2,66 €/Stk.

Jetzt **HIER** bestellen – exklusiv mit BVD-Rabatt:
www.datenschutz-aktuell.de/mib-bvd/

INDIVIDUALISIEREN
Sie Ihre Infobroschüre mit Ihrem eigenen Firmenlogo und den Kontaktdaten des Datenschutzbeauftragten! Bestellen Sie Ihre individualisierte Broschüre einfach per Mail: mib@datenschutz-aktuell.de

Datenschutzrechtlicher Pflichthinweis: Verantwortlicher ist: Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Str. 2-4, 53177 Bonn, Tel: 0228 – 8205-0, E-Mail: info@vnr.de. Unseren Datenschutzbeauftragten erreichen Sie unter der o.g. Anschrift sowie unter Tel: 0228 – 9550 66004, E-Mail: Datenschutzbeauftragter@vnr.de. Weitere Informationen zum Datenschutz erhalten Sie auf unserer Internetseite www.vnrag.de/datenschutz oder auf Nachfrage von uns. Wir halten Sie zu eigenen ähnlichen Produkten per E-Mail auf dem Laufenden (Art. 6 (1) (f) DS-GVO, § 7 Abs. 3 UWG. Wenn Sie das nicht wünschen, können Sie der Zusendung jederzeit (z.B. an die genannten E-Mail-Adressen) widersprechen.

DIE DATENSCHUTZAUFSICHT - HANDELN MIT SCHARFER KLINGE

Maria Christina Rost

Die deutschen Datenschutzaufsichtsbehörden haben durch die seit Mai 2018 geltende Datenschutz-Grundverordnung (DS-GVO) eine der zentralen Neuerungen der europäischen Datenschutzreform erfahren. Mit der DS-GVO wurde das System des Vollzugs- und der Durchsetzungsmittel für Maßnahmen der Datenschutzaufsicht sowie die Rolle der Sanktionen deutlich gestärkt. Die Aufsicht setzt europaweit geltendes Recht durch und wird dadurch quasi zur „europäischen Vollzugsbehörde".

Will und muss man mit der Aufsicht die Klingen streichen, ist es ratsam, einen Überblick über die aufsichtsbehördlichen Maßnahmen bei Verstößen gegen die DS-GVO zu haben. Die Vollzugs- und Sanktionsmaßnahmen der Aufsichtsbehörde führen sonst zu Unsicherheit und Beunruhigung bei den von den Maßnahmen Betroffenen. Für den internen und externen Datenschutzbeauftragten sind gerade die Geldbußen ein gewichtiges Argument gegenüber der Vorstandsebene im Unternehmen, dem Datenschutz die erforderliche und angemessene Aufmerksamkeit zu widmen.

Die zentralen Normen sind Artt. 58 und 83 DS-GVO. Art. 58 DS-GVO regelt die Befugnisse der Aufsichtsbehörde. Diese setzen sich zusammen aus Untersuchungsbefugnissen (Art. 58 Abs. 1 DS-GVO), aus Abhilfebefugnissen (Art. 58 Abs. 2 DS-GVO) als Reaktion auf Verstöße und aus Genehmigungsbefugnissen (Art. 58 Abs. 3 DS-GVO).

I. Abhilfebefugnisse

Zentrale Norm der Befugnisse (powers) der Aufsicht sind die Abhilfebefugnisse in Art. 58 Abs. 2 DS-GVO. Mit den Abhilfebefugnissen (corrective powers) wird das Ziel verfolgt, die Einhaltung der DS-GVO zu sichern. Die Aufsichtsbehörde hat gem. Art. 57 Abs. 1 Buchstabe u) DS-GVO die Pflicht, interne Verzeichnisse über Verstöße gegen diese Verordnung und über gem. Art. 58 Abs. 2 DS-GVO ergriffene Maßnahmen zu führen. Diese teilen sich auf in Befugnisse, die man vor Feststellung eines Verstoßes gegen die DS-GVO hat und in solche Maßnahmen, die die Aufsichtsbehörde ergreifen kann, sofern ein Verstoß gegen die DS-GVO festgestellt wird.

1. Warnung

Im Vorfeld eines Verstoßes kann die Aufsichtsbehörde gem. Art. 58 Abs. 2 Buchstabe a DS-GVO einen Verantwortlichen oder einen Auftragsverarbeiter warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DS-GVO verstoßen. So kann die Aufsichtsbehörde von einem geplanten Projekt erfahren, bei dem Daten verarbeitet werden sollen, welches aber mit den Anforderungen der DS-GVO nicht in Einklang zu bringen ist, weil beispielsweise die TOM, die technisch-organisatorischen Maßgaben, nicht eingehalten werden. In diesem Fall würde der Verantwortliche ein Schreiben von der Aufsicht erhalten, welches die Warnung enthält, dass ein Verstoß nach DS-GVO im Raume steht, wenn der Verantwortliche wie geplant verfährt. Wenn der Verantwortliche oder Auftragsverarbeiter dann dennoch handelt, wirkt sich dieses Verhalten in einem späteren Bußgeldverfahren erschwerend aus.

2. Festgestellter Verstoß gegen die DS-GVO

Stellt etwa die Aufsichtsbehörde bei einer Prüfung infolge einer Beschwerde fest, dass ein Verstoß gegen die DS-GVO vorliegt, kann sie zum einen Maßnahmen ergreifen, die die Wiederherstellung eines DS-GVO-konformen Zustand zum Ziel haben. Die Aufsichtsbehörde kann aber auch anstatt oder zusätzlich Sanktionen aussprechen.

a) Maßnahmen

Die Aufsichtsbehörde kann nach Art. 58 Abs. 2 Buchstaben c-h und j DS-GVO Korrekturmaßnahmen verhängen. Die DS-GVO macht der Aufsicht hierzu Vorgaben. Die Maßnahmen müssen unparteiisch, gerecht, und innerhalb einer angemessenen Frist ausgeübt werden. Jede Maßnahme muss geeignet, erforderlich und verhältnismäßig sein, wobei die Umstände des jeweiligen Einzelfalls zu berücksichtigen sind und das Recht einer jeden Person, gehört zu werden, bevor eine individuelle Maßnahme getroffen wird, die nachteilige Auswirkungen auf diese Person hätte. Überflüssige Kosten und übermäßige Unannehmlichkeiten für die Betroffenen sind zu vermeiden. Weitere Ausführungen hierzu finden sich in Erwägungsgrund 129 zur DS-GVO. Diese Anforderungen zeigen Grenzen aufsichtsbehördlichen Handels auf und bieten zugleich Ansatz zur Verteidigung.

Art. 58 Abs. 2	Korrekturmaßnahmen der Datenschutzaufsichtsbehörde
Buchstabe c	Anweisung, den Anträgen der betroffenen Person in Ausübung der ihr nach dieser Verordnung zustehenden Rechte zu entsprechen
Buchstabe d	Anweisung des Verantwortlichen oder des Auftragsverarbeiters, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen
Buchstabe e	Anweisung des Verantwortlichen, die von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person entsprechend zu benachrichtigen
Buchstabe f	Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung, einschließlich der Verhängung eines Verbots
Buchstabe g	Anordnung der Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung gemäß Artikeln 16, 17 und 18 und die Unterrichtung der Empfänger, an die diese personenbezogene Daten gemäß Artikel 7 Abs. 2 und Artikel 19 offengelegt wurden
Buchstabe h	Widerruf einer Zertifizierung oder die Anweisung der Zertifizierungsstelle, eine gemäß Artikel 42 und 43 erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden
Buchstabe j	Anordnung der Aussetzung der Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation

b) Sanktionen

Im Interesse einer konsequenteren Durchsetzung der Vorschriften der DS-GVO sieht die DS-GVO in Erwägungsgrund 148 Satz 1 vor, dass bei Verstößen gegen die DS-GVO zusätzlich zu den geeigneten Maßnahmen, die die Aufsichtsbehörde gemäß der DS-GVO verhängt, oder anstelle solcher Maßnahmen, Sanktionen einschließlich Geldbußen verhängt werden. Das Schwert kann bisweilen eine sehr scharfe Klinge haben. Verstöße können zur Verwarnung und oder zur Geldbuße führen. Das bedeutet, wenn eine Aufsichtsbehörde einer Firma X gegenüber eine Anweisung erlassen hat, beispielsweise einem Kunden die gewünschte aber bisher verweigerte Auskunft nach Art. 15 DS-GVO zu ▸

AUFSICHTSBEHÖRDE

erteilen, heißt es noch lange nicht, dass dem nicht eine Sanktion in Form einer Verwarnung oder eines Bußgeldes folgt.

aa) Verwarnung

Die Aufsichtsbehörde kann zum einen den Verantwortlichen oder einen Auftragsverarbeiter gem. Art. 58 Abs. 2 Buchstabe b DS-GVO verwarnen, wenn er mit Verarbeitungsvorgängen gegen die DS-GVO verstößt. Die Maßnahme ist ein Verwaltungsakt und es ist nicht ausgeschlossen, dass in der Angelegenheit, wenn es sich beispielsweise um einen weiter andauernden Verstoß handelt, in der nächsten Stufe ein Bußgeld folgt. Diese Form einer Verwarnung ist neu. Das deutsche Ordnungswidrigkeitenrecht kennt die Verwarnung, die an ein Verwarngeld (5 - 55 €) geknüpft ist, sowie die, die ohne Verwarngeld ausgesprochen wird. Der Anwendungsbereich der Verwarnung ist durch Erwägungsgrund 148 Satz 2 näher beschrieben.

Die Entscheidung über die Wahl der Sanktion Verwarnung oder Bußgeld sollte dem Kriterienkatalog aus Art. 83 Abs. 2 DS-GVO Rechnung tragen (Erwägungsgrund 148 DS-GVO). Für das Unternehmen bedeutet dies, dass dieser Katalog dem Unternehmen im Falle eines Verstoßes gegenwärtig und bekannt sein sollte. Erwähnenswert ist in diesem Kontext das österreichische Datenschutz-DeregulierungsG 2018 (beschlossen im NR am 20.04.2018), welches § 11 DSG Österreich ändert. Dort soll die Datenschutzbehörde den Katalog des Art. 83 Abs. 2 bis 6 DS-GVO so zur Anwendung bringen, dass die Verhältnismäßigkeit gewahrt wird. Insbesondere bei erstmaligen Verstößen wird die Datenschutzbehörde im Einklang mit Art. 58 DS-GVO von ihren Abhilfebefugnissen insbesondere durch Verwarnen Gebrauch machen. Für die deutsche Praxis gibt es eine solche Regelung nicht.

bb) Geldbuße

Anstatt einer Abhilfemaßnahme, zusätzlich zu einer Abhilfemaßnahme und trotz einer Verwarnung kann die jeweils zuständige Aufsichtsbehörde ein Bußgeld gem. Art. 58 Abs. 2 Buchstabe i) i.V.m. Art. 83 DS-GVO aussprechen. Die mögliche Bußgeldhöhe, die Anzahl der Bußgeldtatbestände und die Zumessungsanforderungen sind gegenüber der Rechtslage vor dem 25. Mai 2018 deutlich verändert.

Nach Art. 83 Abs. 1 DS-GVO muss die Aufsichtsbehörde darauf achten, dass die Geldbußen gem. Art. 83 für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sind.

Die Tatbestände sind in drei Absätze aufgeschlüsselt. Der Katalog der Bußgeldtatbestände wurde im Vergleich zu vorher um ein Vielfaches erhöht.

Verstöße nach Absatz 4 können mit einem Bußgeld von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden, je nachdem, welcher der Beträge höher ist. Zu diesen Tatbeständen zählen unter anderem der Verstoß gegen Art. 33 DS-GVO, beispielswiese die Nichtmeldung einer Datenpanne.

Verstöße gegen die in Absatz 5 benannten Bestimmungen können mit einem Bußgeld bis zu 20 000 000 EUR oder im Fall eines Unternehmens mit einem Bußgeld von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt werden. Darunter fällt beispielsweise die Nichtachtung der Rechte der betroffenen Personen gemäß Artt. 12 bis 22 DS-GVO, also z.B. die Missachtung eines berechtigten Auskunftsersuchens nach Art. 15 DS-GVO. Wer die berechtigten Maßnahmen der Datenschutzaufsichtsbehörde nach Art. 58 Abs. 2 DS-GVO missachtet, muss gem. Art. 83 Abs. 6 DS-GVO mit einem Bußgeld in der Höhe von Absatz 5 rechnen.

Der immensen Höhe des möglichen Bußgeldes ist es geschuldet, dass die Datenschutzaufsichtsbehörde eine sorgfältige Zumessung vorzunehmen hat. Anleitung hierzu gibt neben Art. 83 Abs. 1 der Kriterienkatalog in Abs. 2. Die Merkmale lassen sich aufschlüsseln in täter- und tatbezogene Merkmale.

II. Herausforderung Harmonisierung

Der europäische Gesetzgeber hat sich bewusst für ein dezentrales System entschieden und gerade nicht eine zentrale europäische „Superbehörde“ institutionalisiert. Damit die Aufsichtsbehörden ihre Aufgaben europaweit harmonisiert ausführen können, sind sie nunmehr in ein europaweites System der Aufsichtsbehörden eingebunden, welches durch den Europäischen Datenschutzausschuss (EDSA = European Data Protection Board = EDPB) zentral gebündelt wird. Ausgestaltet ist dies mit Hilfe von Verfahren der Zusammenarbeit und der Kohärenz. Letztere sind interne Abstimmungsverfahren, die relativ wenig Außenwirkung haben. Damit das dezentrale System der europaweiten Aufsicht effektiv arbeiten kann und damit das sog. Forum-Shopping vermieden wird, ist es nunmehr an dem EDSA gem. Art. 70 Abs. 1 Buchstabe k) DS-GVO Leitlinien zu entwerfen und zu verabschieden. Erste Leitlinien zu dem Bußgeldverfahren gibt es im WP 253. Bezogen auf den hier beschriebenen Kontext müssen nun noch unter anderem Leitlinien zu Art. 58 Abs. 1, 2, und 3 sowie für die Festsetzung von Geldbußen i.S.d. Art. 83 Abs. 2 verfasst werden.

III. Fazit

Auch wenn es solche Leitlinien noch nicht gibt, ist es nicht ratsam, sich mit dem Wissen zurück zu lehnen, dass die Rahmenbedingungen i.S.d. Art. 70 DS-GVO noch geschaffen werden müssen und manch ein unbestimmter Rechtsbegriff der Auslegung durch die Gerichte bedarf. Die Datenschutzaufsichtsbehörden haben zulässiger Weise mit der Verfolgung und Bebußung von Verstößen gegen die DS-GVO begonnen.

Über die Autorin

Maria Christina Rost
Regierungsdirektorin beim Hessischen Beauftragen für Datenschutz und Informationsfreiheit (HBDI)

Anzeige

GESELLSCHAFT

NEUE VERFÜGUNGSRECHTE AN DATEN - EIGENTUM ALS CHANCE ODER RISIKO?

Prof. Dr. Anne Riechert

Ein Eigentumsrecht an Daten wird kontrovers diskutiert. Gesetzlich verankert ist ein solches Recht nicht und es soll durch analoge Anwendung der existierenden gesetzlichen Regelungen auch nicht hergeleitet werden können.[1] Ein Ausschließlichkeitsrecht wird nur an körperlichen Gegenständen anerkannt. Definiert wird als Gegenstand alles, was „als abgrenzbares Etwas außerhalb der Person besteht",[2] wobei dies für personenbezogene Daten verneint wird.[3] Die Einordnung von Daten als immaterielles Gut soll nach überwiegender Rechtsauffassung ebenfalls nicht möglich sein, da im Immaterialgüterrecht nur bereits gesetzlich geregelte Fälle anerkannt werden.[4]

Ein Eigentumsrecht an Daten bedarf daher entweder einer (noch zu schaffenden) gesetzlichen Grundlage oder der richterlichen Rechtsfortbildung. Auch ein im Auftrag des Bundesministeriums für Verkehr und Infrastruktur in Auftrag gegebenes Mobilitätsgutachten schlägt als eine Option ein Eigentumsrecht vor, wobei letztendlich jedoch offen gelassen wird, ob dies eine tragfähige Alternative darstellt. Nach diesem Vorschlag erfolgt die Zuordnung an den wirtschaftlichen berechtigten Datenersteller.[5] Doch welche Chancen und Risiken würde ein solches Recht mitbringen? Ist es nicht entbehrlich, da der Datenmarkt auch ohne ein Dateneigentum ausgezeichnet floriert?

Kritische Stimmen warnen vor den Gefahren einer Monopolbildung und der Monopolisierung von Kundenbeziehungen. So wird vor allem aus ökonomischer Sicht stets darauf verwiesen, dass Zugangsrechte zu Daten wichtiger seien als die Regelung eines Eigentumsrechts. Allerdings besteht oftmals das Missverständnis, dass mit Eigentum zwangsläufig auch eine Monopolstellung verbunden sein müsse. Bereits die Regelungen des Urheberrechts belegen jedoch, dass gesetzlich geregelte Ausschließlichkeitsrechte nicht dazu führen, sämtliche an der Datennutzung Interessierte von der Nutzung auszuschließen. Das Urheberrecht zeige – so argumentiert *Buchner* – dass selbst klassische Ausschließlichkeitsrechte genügend Spielraum eröffneten, um eine Balance des zwischen Ausschließlichkeitsrechten des Rechtsinhabers einerseits und den Freiheits- und Kommunikationsinteressen der Allgemeinheit andererseits herzustellen.[6] Es bleiben daher auch die Ergebnisse der von der Bundesregierung eingesetzten Datenethikkommission abzuwarten, die in diesem Zusammenhang unter anderem die Frage klären sollen, welche Auswirkungen bestehende Zugriffs- und Ausschließlichkeitsrechte an Daten für Wettbewerb und Innovation haben, und welche Folgen zusätzliche Zugriffs- und Ausschließlichkeitsrechte an Daten hätten.[7]

Zu berücksichtigen ist: Die Anerkennung eines Eigentumsrechts an Daten bildet lediglich die Basis und würde weitere Regelungen erfordern.[8] Der Eigentumsbegriff ist normgeprägt und muss vom Gesetzgeber ausgestaltet werden, so dass in diesem Rahmen die Sozialbindung des Eigentums ebenso beachtet werden kann wie die notwendigen und geforderten Zugangsrechte. Hierzu hat das Bundesverfassungsgericht entschieden, dass Inhalt und Funktion an die gesellschaftlichen und wirtschaftlichen Verhältnisse angepasst werden müssen.[9] Es ist also Sache des Gesetzgebers, ein interessengerechtes Regelwerk zu gestalten. Hier können grundsätzlich verschiedene Interessen im Fokus stehen und beispielsweise geprüft werden, ob es u.a. im Hinblick auf maschinengenerierte Daten denkbar wäre, „eine Leistung" beim Eigentum zu belohnen. Gleichzeitig könnten Lösungen für einen angemessenen Zugang zu den Daten diskutiert und geschaffen werden, um den neuen Herausforderungen gerecht zu werden.

Weitere Möglichkeiten beziehen sich auf eine angemessene Partizipation an der vorhandenen Datenbasis, etwa in Form einer Datenagentur, die repräsentativ die Rechte der Bürger wahrnimmt.[10] In diesem Sinne werden außerdem Treuhandmodelle genannt[11] und gleichermaßen aus ökonomischer Sicht eine intensivere Forschung zu Datenkooperativen, Treuhändern oder Datengenossenschaften gefordert.[12] Diese Modelle können ebenso als Antwort auf eine längst bestehende Realität betrachtet werden: Daten sind generiert, sie sind „in der Welt" und das Rechtssystem muss eine interessengerechte Lösung finden, die auch eine Teilhabe derjenigen beinhalten kann, die die Daten erzeugt haben. In diesem Zusammenhang sind insbesondere die Schwierigkeiten der Wertbemessung von Daten zu berücksichtigen. So wird auf den „bewusst blinden Fleck" des europäischen Datenschutzrechts und einem bewussten Nicht-Wahrnehmen der Marktgängigkeit von personenbezogenen Daten Bezug genommen.[13]

Insgesamt würde die grundsätzliche Anerkennung eines Eigentumsrechts an Daten aus rechtlicher Sicht folglich nicht den Auffassungen entgegenstehen, die eine Monopolbildung befürchten, da erst auf einer weiteren Stufe die einzelnen Rechte zu klären sind.[14] Auch die Forderung von Zugangsrechten steht aufgrund der Berücksichtigung des Allgemeinwohls dazu nicht im Widerspruch. Die Befürworter eines Dateneigentumsrechts verweisen auf eine damit verbundene Rechtssicherheit und Rechtsklarheit. Denn die Alternative wären Zugangs- oder Nutzungsrechte an bereits bestehenden Datenbeständen, deren Legitimation sich aufgrund faktischer Zugriffsmöglichkeiten begründet. Faktizität als Rechtsgrundlage? In der Praxis wäre es zwar möglich, Zugangsrechte an Datenbeständen einzuräumen. Rechtsklarheit schafft jedoch die vorherige Entscheidung, ob und auf welcher Legitimationsgrundlage die exklusive und tatsächliche Kontrolle eines Anbieters über Daten begründet sein kann, die auf seinen proprietären Systemen liegen, oder inwieweit ein ausschließliches Zugangs- bzw. Nutzungsrecht einzuschränken ist.

Zu bedenken ist allerdings, dass mit der Anerkennung eines Eigentumsrechts an Daten noch nicht die Frage des Verbraucherschutzes geklärt ist. Hier wäre vielmehr ein paralleles gesetzgeberisches Tätigwerden erforderlich, um die notwendige Vertragsgerechtigkeit herzustellen.[15] Somit wäre ein Eigentumsrecht an Daten lediglich ein Teil einer umfassenderen Datenrechtsordnung in einer neuen digitalisierten Realität, die gleichermaßen Aspekte des Verbraucherschutzes reguliert.

Über die Autorin

Prof. Dr. Anne Riechert

Ist wissenschaftliche Leiterin der Stiftung Datenschutz und Professorin an der Frankfurt University of Applied Sciences.

▶ www.stiftungdatenschutz.org

[1] Siehe hierzu auch Bundesministerium für Verkehr und digitale Infrastruktur, Studie zum Thema „Eigentumsordnung für Mobilitätsdaten?" (August 2017), S. 88; abrufbar unter https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/eigentumsordnung-mobilitaetsdaten.pdf?__blob=publicationFile.

[2] Zech, Information als Schutzgegenstand, S. 94 mit Verweis auf die Definition von Beuthien/Schmölz, Persönlichkeitsschutz durch Persönlichkeitsgüterrechte, S. 19.

[3] Zech, Fn. 2, S. 218, 219. Bei persönlichen Daten trennt Zech danach, ob die Persönlichkeitsrechte ablösbar und damit kommerzialisierbar sind (S. 217 ff. und S. 297 ff.). Als ablösbar bewertet er beispielsweise das Recht am eigenen Bild sowie genetische Informationen (S. 297ff. , S. 306).

[4] Kilian, Personenbezogene Daten als schuldrechtliche Gegenleistung, in: Stiftung Datenschutz - DatenDebatten III, S. 199/200.

[5] Siehe Fn. 1, S. 105 ff. Der Skripturakt wird somit um eine wirtschaftliche Betrachtungsweise ergänzt.

[6] Buchner, „Is there a Right to One's Own Personal Data?", in: Zeitschrift für Geistiges Eigentum, Intellectual Property Journal, 416 ff., 417. Siehe auBerdem Buchner, Eigentumsrechte an persönlichen Daten?, DGRI Jahrbuch 2011, Köln 2012, S. 51, 58.

[7] Siehe Leitfragen der Bundesregierung an die Datenethikkommission vom 05.Juni 2018, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/datenethikkommission/leitfragen-datenethikkommission.pdf?__blob=publicationFile&v=1.

[8] Siehe Fezer, Digitales Dateneigentum – ein grundrechtsdemokratisches Bürgerrecht in der Zivilgesellschaft, in: Stiftung Datenschutz - DatenDebatten III, der von der „zweiten Stufe" spricht.

[9] Siehe hierzu BVerfGE 24, 367, 389.

[10] Fezer, Fn.8, bezieht sich auf ein digitales Bürgerdateneigentum, S. 152.

[11] Buchner, Eigentumsrechte an persönlichen Daten?, DGRI Jahrbuch 2011, Köln 2012, S. 51, 58.

[12] Jentzsch, Datenhandel und Datenmonetarisierung: Ein Überblick, in: Stiftung Datenschutz - DatenDebatten III, S. 188, 190.

[13] v. Lewinski, Wert von personenbezogenen Daten, in: Stiftung Datenschutz - DatenDebatten III, S. 215.

[14] Siehe hierzu Fezer, Fn. 8, S. 112.

[15] Siehe Fezer, Fn. 8, S. 111. Der Vorschlag für eine „Europäische Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte" (vom 09.12.2015 - COM (2015) 634 final) hilft hier nur bedingt weiter, da einige Fragen offen bleiben. So kommt *Hofmann* (Richtlinie Digitale Inhalte – Schuldrechtliche Kontextualisierung von Daten als Wirtschaftsgut, in: Stiftung Datenschutz - DatenDebatten III, S. 175) zu dem Ergebnis, dass dem Ansinnen „den Verbrauchern bestimmte einheitliche Rechte zu verleihen" nur bedingt Rechnung getragen werde.

GESELLSCHAFT

FACEBOOK UND DER DATENSCHUTZ – EIN FALL FÜR DAS BUNDESKARTELLAMT?

Prof. Niko Härting

„Das Bundeskartellamt untersagt Facebook die Zusammenführung von Nutzerdaten aus verschiedenen Quellen" hieß es am Donnerstag, den 07.02.2019, in einer Pressemitteilung der Wettbewerbshüter. Es ging um ein Verbot der Zusammenführung von Facebook-Daten mit anderen Daten, die über andere konzerneigene Dienste wie Whatsapp und Instagram oder über den „Gefällt mir"-Button erhoben werden.

Einschätzung des Bundeskartellamtes

Das Bundeskartellamt stützt das Verbot auf eine missbräuchliche Ausnutzung der marktbeherrschenden Stellung auf dem Markt für soziale Netzwerke. Es handele sich um einen Konditionenmissbrauch nach § 19 Abs. 1 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB). Der Stein des Anstoßes sind die Facebook-Datenschutzrichtlinien, die nach Auffassung des Kartellamts gegen die Wertungen der DS-GVO verstoßen.

Die Wettbewerbshüter meinen, dass die Datenschutzverstöße auf die Marktmacht von Facebook zurückzuführen sind. Facebook könne seine Datenpraktiken nur aufgrund der besonderen Marktstellung des Unternehmens am Markt durchsetzen, da die Nutzer nicht ohne Weiteres zu einer Konkurrenzplattform wechseln können.

Die Behörde ist der Ansicht, dass es für eine Zusammenführung von Daten einer Einwilligung des jeweiligen Nutzers bedarf. Art. 6 Abs. 1 Satz 1 lit. b (Vertragserfüllung) und Art. 6 Abs. 1 Satz 1 lit. f DS-GVO kommen aus Sicht der Bonner Beamten als Rechtsgrundlagen nicht in Betracht. Die Vertragserfüllung sei als Rechtsgrundlage eng auszulegen und nicht mit Effizienz und Vorteilen für den Dienst zu begründen. Auf berechtigte Interessen könne Facebook sich aufgrund seiner überlegenen Verhandlungsmacht gegenüber der Nutzer nicht berufen.

Vorrang der Einwilligung?

Das Bundeskartellamt gibt damit zu erkennen, dass es von einem grundsätzlichen Vorrang der Einwilligung ausgeht, ohne dass sich aus der DS-GVO ein Rangverhältnis der Rechtsgrundlagen noch gar ein grundsätzlicher „Einwilligungsvorbehalt" ergibt. Ganz im Gegenteil sprechen gute Gründe dafür, die Einwilligung als schwächste Rechtsgrundlage zu verstehen. Die Einwilligung ist jederzeit frei widerruflich (Art. 7 Abs. 3 Satz 1 DS-GVO) und bei „klarem Ungleichgewicht" (Erwägungsgrund 43 Satz 1 DS-GVO) im Zweifel nicht als „freiwillig" anzusehen und damit unwirksam. Umstritten ist zudem die Tragweite eines Kopplungsverbots (Art. 7 Abs. 4 DS-GVO i.V.m. Erwägungsgrund 43), das besagt, dass jede Einwilligung, die bei Vertragsschluss abgegeben wird, unwirksam ist, wenn sie sich auf Daten erstreckt, die für den jeweiligen Dienst nicht „erforderlich" sind.

Aus den Schwächen der Einwilligung hat Facebook die Konsequenz gezogen auf andere Rechtsgrundlagen auszuweichen. Mit einer solchen Einschätzung steht Facebook keineswegs allein. Auch aus Aufsichtsbehörden hört man immer wieder, dass man bei der Beurteilung der Rechtmäßigkeit einer Datenverarbeitung sehr skeptisch sei, wenn Daten zur Vertragserfüllung nicht gebraucht werden und auch berechtigte Interessen nicht ersichtlich sind. Ohne berechtigte Interessen und ohne einen Vertragsbezug werde man die Frage nach der Freiwilligkeit und Wirksamkeit einer Einwilligung besonders kritisch stellen.

Nicht alle Datenschützer teilen die kritische Sicht auf die Einwilligung. So scheint Google der Tragfähigkeit von Einwilligungen nach wie vor überzeugt zu sein und setzt seit dem Wirksamwerden der DS-GVO sogar verstärkt auf Einwilligungen, die gerne auch wiederholt vom Nutzer eingeholt werden.

Das Kartellamt schlägt sich in seiner Facebook-Entscheidung klar auf die Seite der „Einwilligungsfreunde" und erteilt damit jeglicher Einwilligungsskepsis eine Absage. Ob es der Rechtssicherheit und der Vereinheitlichung des Datenschutzes in Europa dient, wenn eine mächtige, aber fachfremde Behörde bei einem grundsätzlichen Auslegungsstreit in derart radikaler Weise Partei ergreift, darf bezweifelt werden.

Welche „Konditionen" eigentlich?

Es ist im Übrigen fraglich, welche „Konditionen" Facebook eigentlich missbraucht haben soll. Das Kartellamt zieht eine Parallele zwischen AGB und Datenschutzinformationen, verkennt dabei jedoch, dass Facebook zu derartigen Informationen – wie andere Unternehmen auch – verpflichtet ist (Artt. 13 und 14 DS-GVO). Mit den eigenen Datenschutzrichtlinien erfüllt Facebook gesetzliche Aufklärungspflichten. Es handelt sich nicht um AGB oder andere Vertragsbedingungen, die Facebook unter Ausnutzung der eigenen Marktmacht den zähneknirschenden Nutzern aufoktroyiert.

Datenschutzinformationen stellen kein Kleingedrucktes dar, dem der Nutzer mehr oder weniger bewusst beim Vertragsschluss zustimmt. Es geht vielmehr um einseitige Pflichtinformationen, die von keiner Zustimmung des Nutzers abhängig sind. Die Parallele zu AGB und anderen „Konditionen" eines Vertrages ist keineswegs zwingend und äußerst gewagt.

Kompetenzen der Datenschutzaufsicht

UUnterstellt man einmal, dass es tatsächlich DS-GVO-Verstöße gibt, läge es wirklich an der Marktdominanz, dass Facebook diese Verstöße begehen kann? Vieles spricht dagegen. Datenschutzverstöße sind kein Privileg großer Anbieter. Wenn es nur an der Marktmacht von Facebook läge, dass die Nutzer Datenschutzverstöße hinnehmen, ließe sich nicht erklären, weshalb viele Nutzer auch kleineren Anbietern trotz fragwürdiger Datenpraktiken treu bleiben. Unterstellt man zudem, dass Facebooks DS-GVO-Verstöße tatsächlich so massiv sind, wie vom Kartellamt angenommen, hätten die europäischen Datenschutzbehörden versagt. Seit Mai 2018 hätten die Behörden aber mit aller Entschlossenheit gegen solche Verstöße vorgehen und von ihren Untersagungs- und Bußgeldbefugnissen Gebrauch machen können. Wenn ein Unternehmen massive Datenschutzverstöße begeht und ihm dennoch die Kunden nicht davonlaufen, dürfte dies weniger an der Marktmacht des Unternehmens als an Unzulänglichkeiten bei der Durchsetzung der DS-GVO durch die Datenschutzbehörden liegen.

Ausblick

Facebook geht gegen die Entscheidung des Kartellamts gerichtlich vor. Die Beteiligten dürfen sich auf einen jahrelangen Rechtsstreit freuen. Bis die Prozesse abgeschlossen sind, werden sich Facebooks Datenpraktiken nach aller Erfahrung technisch fortentwickeln, sodass man am Ende um historische Sachverhalte streiten wird. Die Datenschutzbehörden werden derweil auf die Zuschauerränge verwiesen. Wem ist mit solchen Verfahren eigentlich geholfen?

Über den Autor

Prof. Niko Härting
ist namensgebender Partner von HÄRTING Rechtsanwälte, Berlin. Er ist Mitglied der Schriftleitung Computer und Recht (CR), ständiger Mitarbeiter vom IT-Rechtsberater (ITRB) und vom IP-Rechtsberater (IPRB) sowie Herausgeber der Zeitschrift PinG – Privacy in Germany. Seit 2012 ist er Honorarprofessor an der Hochschule für Wirtschaft und Recht, an der er seit 1991 Lehrbeauftragter ist. Er ist Autor zahlreicher Publikationen (u.a. Internetrecht, 6. Auflage 2017 und Datenschutz-Grundverordnung, 1. Auflage 2016).

▶ www.haerting.de

HÄRTING

GESELLSCHAFT

FACEBOOKS UNSICHTBARE DATENSAMMLUNG

Miriam Ruhenstroth

Sie sind auf Partnersuche, zum Beispiel bei Tinder? Oder eher bei der Datingbörse Curvy, für Leute mit Kurven, oder beim Dienst Grindr, für Schwule? Sie wollen mit Kwit Ihre Nikotinsucht besiegen, mit forDiabetes Ihre Zuckerkrankheit begleiten oder sich mit einer Gebets-App Ihrem Glauben widmen?

All diese und die im Folgenden genannten Angebote haben zwei Dinge gemeinsam. Erstens: Die meisten Nutzer greifen per Smartphone-App darauf zu. Und zweitens: Jede dieser Apps meldet sich bei Facebook, sobald man sie öffnet.

Zu diesem Ergebnis kommen zwei Studien, die im November und Dezember 2018 unabhängig voneinander von mobilsicher.de und der gemeinnützigen Organisation Privacy International veröffentlicht wurden.

Mobilsicher.de hatte dazu gezielt 13 Apps aus den Bereichen Religion, Gesundheit, Sexualität und Politik getestet, die das kritische Facebook-SDK enthielten. Getestet wurden die Android- und die iOS-Varianten.

Privacy International hatte eine Auswahl von insgesamt 34 Android-Apps getestet, von denen 23 beim Start Kontakt zu Facebook aufnahmen.

Facebook schätzt Interessen anhand genutzter Apps ein

Facebook sammelt auf diesem Weg wertvolle Informationen außerhalb der eigenen Plattform: Wer benutzt welche Apps und wann?

Das mag bei einer Foto- oder Wetter-Anwendung unproblematisch sein – wer sich aber mit der Bibel + Audio-App dem christlichen Glauben widmet oder sich per Muslim Pro an die muslimischen Gebetszeiten erinnern lässt, gibt viel über sich preis.

Mit diesen Informationen füttert Facebook seine Nutzerprofile und macht sie so zu Geld. Wer sich bei der App „Indeed" für die Jobsuche angemeldet hat, wird sich eventuell für Bewerbungstrainings interessieren, wer mit der App Migraine Buddy seine Kopfschmerzen protokolliert, reagiert vermutlich gut auf Werbung für neue Migräne-Mittel.

Entwickler bauen Facebook-Baustein in ihre Apps ein

Die Verbindung zu Facebook kommt nicht durch dunkle Machenschaften des Konzerns zustande. Die App-Entwickler bauen sie höchstpersönlich in ihre Apps ein. Facebook stellt dafür einen Software-Baustein zur Verfügung, ein sogenanntes Software Development Kit (SDK). Es ist fertig programmiert und muss nur noch heruntergeladen und eingebaut werden.

Warum nutzen die Entwickler diesen Baustein? Die meisten Menschen kennen Facebook nur als Plattform, um sich mit Freunden auszutauschen – ein Social-Media-Dienst eben. Aber der Konzern hat noch ganz andere Angebote im Portfolio.

Für Anbieter von Apps stellt er zum Beispiel einen Dienst für die Nutzeranalyse zur Verfügung: Facebook Analytics. Mit Facebook Analytics bekommt der Betreiber einer App Auskunft darüber, was Nutzer in der App tun, an welcher Stelle im Menü sie womöglich abbrechen, welche Funktionen sie besonders mögen.

Wichtige und völlig legitime Informationen also, um eine gute App herzustellen.

Daten gegen kostenlosen Service

Der Analyse-Dienst von Facebook ist nicht nur sehr gut, er ist im Gegensatz zu vielen anderen vergleichbaren Diensten auch kostenlos. Entsprechend beliebt ist er.

Das Testsystem der französischen Nichtregierungsorganisation Exodus Privacy fand das Modul für Facebook Analytics in rund 20 Prozent aller 42.675 getesteten Apps. Das Forschungsprojekt AppCensus mit Sitz in Kalifornien untersuchte 83.064 Apps und stellte in rund 30 Prozent davon eine Datenverbindung zu Facebook (Facebook Analytics und alle anderen Facebook-Dienste) fest.

Der Preis für die praktischen Dienste: Die Nutzerdaten, die dabei anfallen, landen bei Facebook. Bei Facebook-Analytics zum Beispiel kann der Entwickler die Daten zwar ansehen, er kann aber nicht darüber bestimmen.

Kaum Problembewusstsein bei Anbietern

Die Bereitschaft der App-Betreiber, sich mit dem Thema zu befassen, ist nicht sehr ausgeprägt.

Von den 23 Unternehmen, die Privacy International vor der Veröffentlichung um eine Stellungnahme gebeten hatte, antworteten bis zum Zeitpunkt der Veröffentlichung nur sieben, nur zwei davon kündigten an, das Facebook-SDK zu deaktivieren.

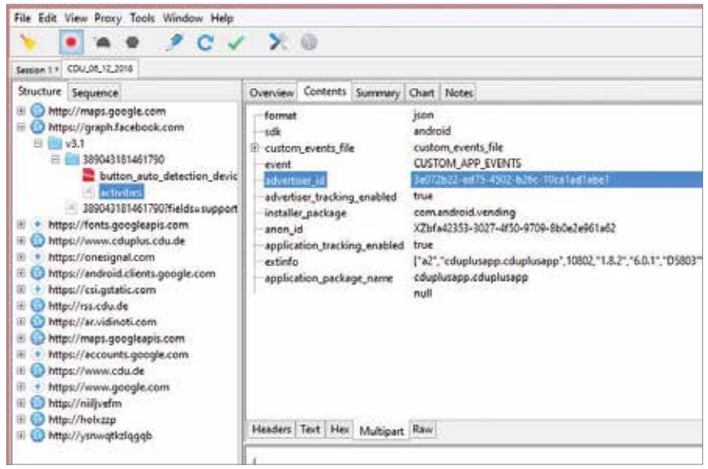
Als Reaktion auf die Untersuchung von mobilsicher.de entfernten vier Anbieter das Facebook-SDK, ein fünfter kündigte dieses zumindest an.

Was genau erfährt Facebook?

Über dieses Arrangement machen sich die Anbieter und Entwickler von Apps offenbar wenig Gedanken. Zum Teil liegt das daran, dass die Betreiber gar nicht genau wissen, was das Facebook-Modul eigentlich tut.

Den wenigsten App-Herstellern ist zum Beispiel klar, dass die Daten, die das Modul aus ihrer App heraus sendet, nicht wirklich anonym sind.

Wenn man den Datenstrom einer App mit integriertem Facebook-Modul analysiert, sieht das typischerweise so aus (hier am Beispiel der App der Partei CDU, „Meine CDU", Version 1.8.2. Die Partei hat das Facebook-Modul nach dem Hinweis auf unsere Untersuchung aus der App entfernt).



Datenverkehr der App Meine CDU. Links im Bild: Zu diesen Internetadressen nimmt die App Verbindung auf, sobald man sie öffnet – noch bevor man auch nur einmal getippt hat. Rechts: Der Inhalt eines der Datenpakete, die an Facebook gehen. Markiert ist die Werbe-ID. Hinweis: Das Facebook-SDK wurde inzwischen aus der App entfernt.

Neben technischen Informationen, zum Beispiel der Modellbezeichnung D5803 für ein Sony Xperia Z3 Compact, erfährt Facebook auch die Uhrzeit, die IP-Adresse und welche App genutzt wird – in diesem Beispiel die offizielle App der Christlich Demokratischen Partei Deutschlands, CDU.

Entscheidend ist aber die markierte Zeile im Bild, bezeichnet mit „advertiser_id". Hier steht als Wert die sogenannte Werbe-ID, in unserem Beispiel die Ziffernfolge „3e072b22-ed75-4502-b26c-10ca1ad1abe1".

Streitfrage: Wie anonym ist die Werbe-ID?

Jedes Android-Handy, das mit einem Google-Konto verknüpft ist, hat eine solche Werbe-ID. Bei iPhones gibt es mit dem „Identifier for Advertising (IDFA)" eine vergleichbare Kennnummer, die das Apple-Betriebssystem iOS erstellt.

Mit „Werbe-ID" ist in der Folge sowohl Apples IDFA als auch Googles Ad-ID gemeint. Beide sind eindeutig. Das heißt: Jedes Handy hat eine andere. Und jede App kann sie ohne weitere ▸

Berechtigung oder Benachrichtigung auslesen.

Das macht sich Facebook zunutze: Wer sich auch nur ein einziges Mal mit seinem Handy bei Facebook einloggt, dessen Werbe-ID wird von Facebook ausgelesen und mit dem eigenen Facebook-Konto verbunden. Wer dort Name, E-Mail-Adresse oder Geburtsdatum hinterlegt hat, ist damit alles andere als anonym.

Fortan kann Facebook jede andere Information, die zusammen mit der Werbe-ID auf seinen Servern landet, dem passenden Nutzerprofil zuordnen. Und genau das tut der Konzern mit den Informationen, die das Facebook-Modul aus Drittanbieter-Apps sendet, wie ein Facebook-Sprecher auf Anfrage von mobilsicher.de bestätigte.

Damit verliert die Werbe-ID bei Facebook ihre Anonymität, so der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Prof. Johannes Caspar, gegenüber mobilsicher.de:

„Anonym sind diese Daten nur, wenn sie keiner konkreten Person zugeordnet werden können, oder wenn dies nur mit unverhältnismäßig großem Aufwand möglich ist. Hier wird aber gerade ein konkreter Personenbezug durch den Abgleich mit vorhandenen Nutzerprofilen bei Facebook hergestellt."

Auch die Tatsache, dass Nutzer die Werbe-ID manuell verändern können, lässt Caspar nicht als Ausrede gelten.

„Wenn schon eine IP-Adresse als ein personenbezogenes Datum angesehen wird, so muss dies auch für eine gerätegebundene Werbe-ID gelten, zumal das jeweilige Gerät regelmäßig von einer Person genutzt wird. Die für ein Gerät eindeutige Werbe-ID kann zwar zurückgesetzt werden, wird dadurch aber durch eine neue eindeutige Nummer ersetzt, die dann wieder mit dem Gerät und damit mit dessen Nutzer fest verbunden ist", so der Datenschutzbeauftragte.

Und weil ohnehin kaum jemand seine Werbe-ID regelmäßig zurücksetzt, funktioniert sie in der Praxis auf jeden Fall hervorragend als Identifikationsmerkmal. Dass sich trotzdem sogar in Apps mit Bezug zu Gesundheit, Religion oder politischer Gesinnung ein Facebook-Modul findet, beweist im besten Fall die Arg- und Ahnungslosigkeit der Entwickler, im schlimmsten ihre Skrupellosigkeit.

Transparenz für Nutzer? Fehlanzeige

Für den Nutzer gibt es keine Möglichkeit zu erkennen, ob eine App Daten an Facebook überträgt. Die Übertragung ist unabhängig davon, ob man sich mit dem eigenen Facebook-Konto in der App anmeldet, und sie findet selbst dann statt, wenn man gar kein Facebook-Konto hat.

Keine der von mobilsicher.de getesteten Apps geben darauf einen expliziten Hinweis per Dialogfenster. Nicht einmal die Hälfte erwähnt das Facebook-Modul in der Datenschutzerklärung.

Strenggenommen ist keine App mit dem Facebook-SDK in der Standardeinstellung mit geltendem Datenschutzrecht vereinbar. Denn dann beginnt die Datenübertragung an Facebook unmittelbar beim Öffnen der App – noch bevor irgendeine Information angezeigt oder abgenickt werden könnte.

Das wäre aber laut Johannes Caspar im Falle einer Übertragung an Facebook mindestens nötig:

„Werden Daten an Dritte übermittelt – hier zum Beispiel durch die Übertragung der Werbe-ID an Facebook – ist dies in der Regel nur mit Zustimmung des Betroffenen möglich. Hierfür bedarf es einer informierten Einwilligung, die gegebenenfalls durch eine nicht gesetzte Checkbox ausgestaltet sein kann, wobei die Übermittlung der Daten erst dann erfolgt, nachdem der Nutzer sie gesetzt hat", erklärt Hamburgs Datenschutzbeauftragter, der in Deutschland für die Kontrolle von Facebook zuständig ist.

Um das zu verhindern, müssten die Entwickler spezielle Veränderungen an dem SDK vornehmen – ein Schritt, den kaum jemand geht.

Facebook selbst bestätigt auf Anfrage, dass Nutzer derzeit nicht sehen können, welche Informationen aus Apps der Konzern mit dem eigenen Profil verknüpft hat. Mark Zuckerberg hatte eine solche Funktion bereits im Mai 2018 angekündigt. Sie soll „Clear History" heißen und ist bis heute nicht verfügbar.

Undurchsichtig: Sind auch Nutzer ohne Facebook-Konto betroffen?

Auf die Frage, was Facebook mit den Informationen von Nutzern ohne Facebook-Konto tut, antwortet das Unternehmen:

„Facebook only processes information as needed and doesn't process or retain information for non-FB users in the same manner that it does for users."

Auf Deutsch: Facebook verarbeitet nur Informationen, die benötigt werden, und verarbeitet und speichert Informationen von Nicht-Facebook-Nutzern anders, als die von Facebook-Nutzern.

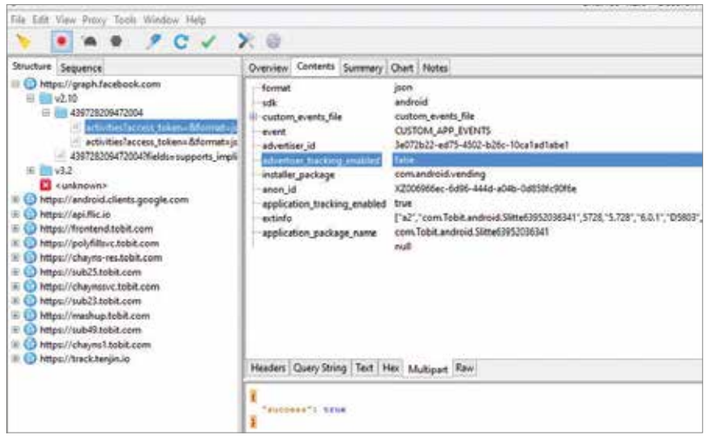
Eine klare Aussage, dass Facebook keine Profile von Nicht-Nutzern anlegt, sieht anders aus. Eine informierte Entscheidung über die eigenen Daten auch.

Gefühlte Wahlmöglichkeiten

Dass Informationen aus Drittanbieter-Apps für personalisierte Werbung verwendet werden, ist keine Vermutung, sondern wurde von Facebook auf Anfrage von mobilsicher.de bestätigt. Auch die Datenrichtlinie von Facebook erklärt es relativ eindeutig in der Sektion „Informationen von Partnern".

Ein Problem sieht Facebook darin nicht, denn, darauf weist der Konzern regelmäßig hin, Nutzer hätten ja die Wahl: Jeder könne sich gegen personalisierte Werbung entscheiden – entweder über eine entsprechende Einstellung im Mobilgerät selber oder im Menü des eigenen Facebook-Kontos. Im Jargon nennt man diese Widerspruchsmöglichkeit „Opt-out".

In der Datenstrom-Analyse lässt sich erkennen, dass in diesem Fall das Facebook-Modul die genannten Informationen genauso überträgt. Allerdings steht dann in dem Feld mit dem Namen „advertiser_tracking_enabled (eine Zeile unter der Werbe-Id) die Angabe „false" – auf Deutsch so viel wie „falsch" oder „nicht zutreffend" (hier am Beispiel der App „SPD Landtagsfraktion NRW" Version 5.728, die vom Dienstleister Tobit Software gehostet wird. Aus der Android-Version wurde das Facebook-SDK inzwischen entfernt).



Datentransfer der App SPD Landtagsfraktion NRW. Die Einstellung personalisierte Werbung deaktivieren im Geräte-Menü wurde angeschaltet. Links im Bild: Zu diesen Internetadressen nimmt die App Verbindung auf, sobald man sie öffnet – noch bevor man auch nur einmal getippt hat. Rechts: Der Inhalt eines der Datenpakete, die an Facebook gehen. In der markierten Zeile advertiser_tracking_enabled steht nun false. Die Daten werden jedoch trotzdem übertragen.

Das Facebook-Modul sendet die Daten also wie gehabt, nur schickt es eine Art Markierung mit, die anzeigt, dass der Nutzer sich gegen personalisierte Werbung entschieden hat.

Auf die Frage, ob die Informationen in diesem Fall nach der Übertragung gelöscht werden, antwortet der Konzern:

„If a person utilizes one of these controls, then Facebook will not use data gathered on these third-party apps (e.g. through Facebook Audience Network), for ad targeting."

Auf Deutsch: Wenn eine Person eine dieser Einstellungen nutzt, wird Facebook die gesammelten Informationen aus Drittanbieter-Apps nicht für personalisierte Werbung nutzen.

Die Zweideutigkeit dieser Antwort ist gar nicht zu übersehen und lässt im Grunde nur einen Schluss zu: Facebook sammelt die Daten trotzdem. Sollte ein Nutzer irgendwann seine Einstellung ändern und personalisierte Werbung wieder zulassen, wäre vermutlich ein vollständiges Interessensprofil vorhanden und einsatzbereit. ▸

Wie kann man sich schützen?

Unter Android empfehlen wir, vor der Installation zu prüfen, ob eine App Facebook eingebunden hat. Das ist zum Beispiel in der Datenbank der gemeinnützigen Organisation Exodus Privacy oder des Forschungsprojektes AppCensus zu sehen. Blockieren können Sie den Datenstrom mit verschiedenen Apps.

Wir empfehlen zum Beispiel die App „Blockada“, betrieben von Freiwilligen um den schwedischen Entwickler Karol Gusak. Das Projekt ist spendenfinanziert, der Quellcode ist offen für jeden zugänglich und im F-Droid erhältlich.

Unter iOS sieht es mit der digitalen Selbstverteidigung schon schwieriger aus. Hier gibt es keine Datenbank mit getesteten Apps, in der man Informationen vor der Installation nachschlagen könnte. Auch eine App zum Blockieren einzelner Datenströme können wir derzeit nicht empfehlen.

App-Name	Android, 28.11.2018	iOS, 05.01.2019	Reaktion
Moodpath (Depressionsbegleiter)	Facebook-Verbindung beim Start	SDK entfernt	SDK aus Android und iOS entfernt
Bible + Audio (Gebets-App)	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
MuslimPro (Gebets-App)	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
For Diabetes	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
OKCupid (Dating)	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
Curvy (Dating für Leute mit Kurven)	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
Grindr (Dating für Schwule)	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
Meine CDU	Facebook-Verbindung beim Start	SDK entfernt	SDK aus Android und iOS entfernt
SPD Landtagsfraktion NRW	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	SDK aus Android entfernt
MigraineBuddy	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	keine
Kwit	Facebook-Verbindung beim Start	Facebook-Verbindung beim Start	Revision angekündigt
Schwangerschaft+	Facebook-Verbindung beim Start	SDK entfernt	SDK aus Android und iOS entfernt

Über die Autorin

Miriam Ruhenstroth
leitet die Redaktion von mobilsicher.de, einem unabhängigen Informationsangebot zu Datenschutz und Sicherheit bei Mobilgeräten. Davor arbeitete sie viele Jahre als freie Technik- und Wissenschaftsjournalistin. Sie lebt und schreibt in Berlin.

▶ https://mobilsicher.de

DAME 2018: „DATENSCHUTZ IST IN DER GESELLSCHAFT ANGEKOMMEN“

Jury nominiert drei Produktionen für BvD-Medienpreis 2018

Die Anforderungen steigen nicht nur im Datenschutz. Auch die Jury der zweiten Ausgabe des Datenschutz Medienpreises DAME des BvD war gefordert: 39 Einreichungen sichteten die sechs Datenschutz-Experten und die Vorjahresgewinnerinnen in diesem Jahr; bei der ersten Ausgabe im vergangenen Jahr waren es 25 Einreichungen gewesen. Entsprechend spannend verlief die Jury-Sitzung. Nach ausführlicher Diskussion nominierten sie das ZDF-Kinder- und Jugendportal „App+on“ von Redakteurin Nadja Kronemeyer, den Song „Spiel mit offenen Daten“ von Musikkabarettist Alex Döring sowie den Kurzfilm „Chancen und Risiken von Gesundheitsdaten“ der Multimedia-Studentin Meret Kaufmann.

Das Votum der Jury wertete BvD-Vorstandsvorsitzender Thomas Spaeing als „einen guten Querschnitt“ aller Einreichungen. Bei fast 40 Beiträgen fiel der Jury allerdings die Abstimmung nicht leicht. „Meine Favoriten haben es nur teilweise in die Endrunde geschafft“, sagte Spaeing. Aber einer davon, der Kurzfilm zu Gesundheitsdaten, ist unter den Nominierten. „Zum einen greifen solche Beiträge die Problematik auf, geben aber gleich eine Anleitung oder Erklärung. Kurz und in der Sprache der Zielgruppe“, sagte er. „Wenn wir mit der DAME zu solchen Formaten anregen, dann hat der Preis seinen Zweck erfüllt.“

Barbara Thiel: „Wachsendes Interesse am Thema Datenschutz“

Eine Reihe von Beiträgen befassten sich mit der Datenschutz-Grundverordnung (DS-GVO), manche Wettbewerbsproduktionen kamen auf über 30 Minuten, ein Theater- und Tanzstück war dabei, viele Erklärfilme, wie sie bei der ersten DAME 2017 in der Endrunde vertreten waren, und eine Reihe von Radio-Beiträgen. Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen, hatte es eine Hörfunk-Produktion über die IT-Unternehmerin Yvonne Hofstetter angetan, die mit ihren datenkritischen Bestsellern für Aufsehen sorgt. „Der war für mich von Anfang bis Ende unglaublich spannend“, sagte Thiel.

Insgesamt beeindruckte sie die Vielfalt der Einreichungen und die gestiegene Zahl der Medienproduktionen zum Thema Datenschutz. „Das zeigt, dass es ein wachsendes Interesse am Thema Datenschutz gibt“, sagte sie. Insbesondere Jüngere entwickelten ein Bewusstsein dafür, dass persönliche Daten nicht sorglos weitergegeben und geteilt werden sollten. „Dass ein solcher Datenverzicht auch sehr humorvoll im Wege einer Datendiät praktiziert werden kann, hat mir ausgesprochen gut gefallen.“

Frederick Richter: „In der Gesellschaft angekommen“.

Auch Frederick Richter, Vorstand der Stiftung Datenschutz, wertet den Facettenreichtum der Beiträge als Erfolg: „Das Thema Datenschutz ist in der Gesellschaft angekommen“, sagte er. Ihn begeisterte vor allem die Songs, die sich um die DAME 2018 bewarben, und von denen es „Spiel mit offenen Daten“ in die Endrunde schaffte.

„Wie man mit Gitarre oder Ukulele die vermeintlich nüchternen Themen Datenschutz, Umgang mit persönlichen Daten und Datenüberwachung witzig vertonen kann, das fand ich toll“, sagte er. Aber auch die Professionalität einer Reihe von YouTuber- und Influencer-Filmen habe ihn beeindruckt. „Die Beiträge unterscheiden sich meiner Meinung nach kaum mehr von professionellen TV-Produktionen.“

Birgit Kimmel: „Authentisches Format“

Birgit Kimmel, die pädagogische Leiterin von klicksafe.de, freut sich, dass ihr Favorit „App+on“ in der Schlussrunde ist, „weil die Plattform unter anderem Lösungsstrategien für Probleme und Sorgen humorvoll und ▸

AUS DEM VERBAND

anschaulich von jungen Protagonistinnen und Protagonisten vermittelt". Für Kimmel ist „App+on" „ein sehr gelungenes, authentisches Format".

Klaus Müller: „Datenschutz aus dem Leben gegriffen"

Für Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands (vzbv), fand die Jury mit den Nominierten am Ende eine „gute, spannende Auswahl". Ihn begeisterte, „dass Datenschutz nicht verquarst, wissenschaftlich oder politisch kompliziert rüberkommt, sondern aus dem Leben gegriffen ist". Das machten auch die drei Nominierten deutlich.

Sebastian Sprenger: „Ganz tolle Sache"

Neu in der Jury war Sebastian Sprenger von der DATEV-Stiftung Zukunft, die den Datenschutz Medienpreis seit November 2018 unterstützt. Beeindruckt hat ihn unter anderem ein Kunstprojekt über die Zusammenführung von biometrischen Passphotos in Reisepässen, dass er über die 30 Minuten hinweg „extrem spannend" fand. „Eine ganz tolle Sache" aber ist auch für Sprenger das nominerte Medienportal „App+on". Die vielen Kurzfilme auf der Seite lüden Kinder und Jugendliche ein, sich in das Thema Datenschutz einzuklinken und mit Gleichaltrigen oder Eltern darüber zu diskutieren.

Auch die Gewinnerinnen der DAME 2017, Monica Oliveira, Natalia Rasstrigina und Leslie Iseli gaben per Videobotschaft aus der Schweiz jeweils ihre Favoriten der Jury mit auf den Weg. Die drei, die mit dem Video-Clip „Social Engineering" im vergangenen Jahr die mit 3.000 Euro dotierte DAME-Auszeichnung gewannen, waren von der Vielfalt begeistert.

Monica Oliveira: „Wirklich umgehauen."

„Manche haben mich wirklich umgehauen", sagte Oliveira. Natalias Favorit, ein Rap-Video der Jugend-Beratung Juuuport e.V. aus Oldenburg hat es nicht unter die Nominierten geschafft. Komponist und Sänger Kevin Lehmann, einer der Juuuport-Scouts, die Jugendliche bei Online-Problemen wie Mobbing beraten, dürfte jedoch kaum enttäuscht sein. Er erhielt im vergangenen Jahr für sein Video „Datenschutz unter Artenschutz" den mit 500 Euro dotierten Sonderpreis Jugend der Internet-Initiative klicksafe. Zudem hatte der BvD mit Unterstützung der DATEV-Stiftung Zukunft mit ihm 2018 ein professionelles Video dazu gedreht.

Wer bei der DAME-Auszeichnung 2018 das Rennen macht, entscheidet sich am 5. Juni 2019 in Berlin. Dann wird Moderator Ralph Caspers und BvD-Vorstand Thomas Spaeing mit den Jury-Mitgliedern den Gewinner bei einer feierlichen Preisvergabe küren. Parallel finden am 5. und 6. Juni die BvD-Verbandstage 2019 statt. Sie stehen in diesem Jahr unter dem Motto „Künstliche Intelligenz und Datenschutz: (k)ein Widerspruch?" und beschäftigen sich unter anderem mit autonomem Fahren und Scoring-Algorithmen – Themen, die auch viele DAME-Einreichungen aufgegriffen hatten.

Die Jury des Datenschutz Medienpreises 2018

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

Dr. Sebastian Sprenger
Referent der DATEV-Stiftung Zukunft

Barbara Thiel
Landesbeauftragte für den Datenschutz Niedersachsens

Monica Oliveira
Natalia Rasstrigina und Leslie Iseli, Gewinnerinnen des Datenschutz Medienpreises 2017

Die drei nominierten Beiträge für die DAME 2018

ZDF-Onlinemagazin „App+on. Sicher ins Netz mit Handy und Co.",
verantwortet von Redakteurin Nadja Kronemeyer
https://www.zdf.de/kinder/app-und-on

Song „Spiel mit offenen Daten" von Alex Döring
https://www.dropbox.com/s/unw2pye3dg09tjo/Spiel-mit-offenen-Daten-DAME-DÖRING-FEYRER.mov?dl=0

Kurzfilm „Chancen und Risiken von Gesundheitsdaten" von Meret Kaufmann und Team
https://www.satw.ch/blog/article/2018/09/18/satw-film-gewinnt-video-wettbewerb/

BVD-NEWCOMERFORUM

Jürgen Hartz

Anfang 2018 hat der BvD ein neues Veranstaltungsformat geschaffen.

Mit dem „BvD-Newcomerforum“ sollen, so die Idee, neue Mitglieder über den Berufsverband umfassend informiert, erste Kontakte zu Kollegen hergestellt und vor allem viele Fragen beantwortet werden. Darüber hinaus sollen die Teilnehmer in das Tätigkeitsfeld des Datenschutzbeauftragten und die Rahmenbedingungen eingeführt werden. Auslöser für dieses neue Format war auch der erhebliche Mitgliederzuwachs durch die DS-GVO und der Wunsch diese neuen Mitglieder in den Verband einzubinden

Das neue Veranstaltungsformat fand bereits in Berlin, Frankfurt, Nürnberg und Duisburg statt. Als Referenten fungierten die Vorstände und die Geschäftsstelle. Zunächst wurde der BvD mit seinen Aktivitäten und Gremien dargestellt. Selbst dem einen oder anderen „alten BvDler“ die vereinzelt dabei waren, waren nicht alle Aktivitäten im Verband bekannt. Kurze Fachvorträge stellten Informationen bereit und zeigten beispielsweise wie Datenschutz als Projekt im Unternehmen eingeführt werden kann. Dennoch wurde immer Wert auf hohe Flexibilität im Ablauf gelegt, um den Anforderungen und Wünschen der Teilnehmer nachkommen zu können. Insbesondere wurde Freiraum für Fragen zum Berufsbild, zur Umsetzung bestimmter Aufgaben, zur DSFA und auch der Haftung des DSB berücksichtigt.

Rückblickend kann man sagen, dass es zwar einen Leitfaden für die Referenten gab, aber jede Veranstaltung am Ende anders ablief und geprägt war von der Intensität, mit der sich die Teilnehmer eingebracht haben.

Besonders erfreulich ist es, dass uns die jeweils zuständigen Aufsichtsbehörden unterstützt haben. Bei jeder Veranstaltung konnten wir eine/n Mitarbeiter/in begrüßen, die die Arbeit und Aufgaben der Behörde vorgestellt haben und sich darüber hinaus den Fragen der Teilnehmer gestellt haben. Dafür an diese Stelle nochmals herzlichen Dank.

Weitere Veranstaltungen sind geplant.

Die Termine finden Sie immer auf

▶ www.bvdnet.de

Karsten Dreyer:

> *„Das BvD-Newcomerforum ist eine hervorragende Möglichkeit den BvD mit seinen vielfältigen Möglichkeiten näher kennen zu lernen, ein paar fachliche Infos mitzunehmen und vor allem auch, um persönliche Kontakte zu anderen Datenschützern aufzubauen. Ich kann die Teilnahme jedem Neueinsteiger nur wärmstens empfehlen.“*

Isabel Kaßner:

> *„Das Newcomer-Treffen ist eine gute Kombination aus Netzwerkmöglichkeiten und fachlichem Input. Über die Website vom BvD wurde ich aufmerksam auf das Newcomer-Treffen und das machte mich neugierig: Den Verband kennenlernen und gleichzeitig Gleichgesinnte, das fand ich sehr interessant. Meine Erwartung wurde nicht enttäuscht: für mich eine sehr gelungene Veranstaltung, durch die der Verband ein Gesicht bekommen hat!“*

Über den Autor

Jürgen Hartz
Stellv. Vorstandsvorsitzender
des BvD e. V.

Anzeige

BvD e.V.
DATENSCHUTZ GESTALTEN

Überblick
Seminare – 1. Halbjahr 2019

Termin	Seminar/ Workshop	Ort
04.04.2019	**Datenschutz in der stationären Versorgung**	NH Collection Berlin Mitte Referent: Dr. Bernd Schütze
05.04.2019	**Datenschutz in der ambulanten Versorgung**	NH Collection Berlin Mitte Referent: Dr. Bernd Schütze
08.04.2019	**Der Datenschutzbeauftragte und die Betriebsverfassung**	Novotel Frankfurt City Referent: Dr. Christoph Bausewein
13.05.2019	**Die ePrivacy Verordnung – Seminar**	AZIMUT Hotel Cologne, Köln Referentin: Kristin Benedikt
13. - 14.05.2019	**Die ePrivacy Verordnung – Seminar & Workshop**	AZIMUT Hotel Cologne, Köln Referentin: Kristin Benedikt
14.05.2019	**Die ePrivacy Verordnung – Workshop**	AZIMUT Hotel Cologne, Köln Referentin: Kristin Benedikt
15.05.2019	**Die Datenschutz-Folgenabschätzung**	AZIMUT Hotel Cologne, Köln Referent: Andreas Sachs
04.06.2019	**Sonderseminar – Die Datenschutz-Folgenabschätzung**	ELLINGTON Hotel Berlin Referent: Andreas Sachs
04.06.2019	**Sonderseminar – Die Datenschutzverletzungen, Prüfungen, Bußgeld**	ELLINGTON Hotel Berlin Referent: Dr. Jens Eckhardt, Dr. Stefan Brink
04.06.2019	**Sonderseminar - Datenschutz spannend machen**	ELLINGTON Hotel Berlin Referent: Stefan Purder
04.06.2019	**BvD-Newcomerforum**	ELLINGTON Hotel Berlin Referent: Jürgen Hartz

* nur für BvD Mitglieder

Information und Anmeldung unter www.bvdnet.de

„DATENSCHUTZRECHT - DS-GVO MIT BDSG“

Simitis, Hornung, Spieker (Hrsg.)

Simitis, Hornung, Spieker (Hrsg.)
»Datenschutzrecht - DS-GVO mit BDSG«

Nomos Verlagsgesellschaft Baden-Baden

1.Auflage 2019 / 1.474 Seiten
ISBN-13: 978-3848735907
198,00 Euro

„Den Simitis“ vom Nomos-Verlag wird es auch unter der Datenschutz-Grundverordnung weiterhin geben. War der Standardkommentar für das BDSG der „Platzhirsch“ unter den Großkommentaren, sieht sich der Nachfolger für die Datenschutz-Grundverordnung einer mittlerweile stattlichen Konkurrenz an Kommentaren gegenüber. Das Herausgeberteam wurde erweitert und umfasst nun weitere Wissenschaftler. Auch das Autorenteam unterlag Veränderungen. Bei den Kommentatoren, bestehend u.a. aus aktiven und ehemaligen Leitern und Mitarbeitern von Aufsichtsbehörden, finden sich auch Autoren aus dem Gesetzgebungsverfahren (Jan Philipp Albrecht) und bekannte Vertreter der Wissenschaft.

Die Regelungen des BDSG werden bei den entsprechenden Artikeln der DS-GVO eingearbeitet und berücksichtigt. Dadurch stellen die Kommentierungen eine ganzheitliche Betrachtung der rechtlichen Grundlagen im deutschen Rechtsraum sicher. Für eine Zuordnung der Regelungen des BDSG bei gezielter Suche innerhalb der Kommentierung hilft ein angehängtes Fundstellenverzeichnis.

Die Kommentierungen folgen einem einheitlichen Schema, auch wenn dies jeder Kommentator für sich selbst betitelt: Nach einem Überblick / einer Vorbemerkung und der Entstehungsgeschichte werden die entsprechenden Absätze systematisch erläutert. Gut gelöst wurde die Komplexität der Abbildung von Einzelthemen, die im Text der DS-GVO nicht explizit abgebildet werden, wie Videoüberwachung, Verbraucherkredite, Scoring, Bonitätsauskünften, Werbung, Markt- und Meinungsforschung, die aber trotzdem im Beratungsalltag einen großen Teil der Fragestellungen zur Rechtmäßigkeit ausmachen. Diese Themen werden ausführlich in insgesamt vier Anhängen zu Art. 6 DS-GVO behandelt.

Der Kommentar bietet eine dogmatisch ausführliche Basis für die Befassung mit allen Aspekten der datenschutzrechtlichen Thematiken und ergänzt hervorragend die Sammlung datenschutzrechtlicher Literatur für all diejenigen, die neben den Hinweisen aus der Praxis auch eine ausführliche Darstellung der Hintergründe und Begründungen erwarten.

„BIG DATA UND RECHT – EINFÜHRUNG FÜR DIE PRAXIS“

Calderola / Schrey

Calderola / Schrey
»Big Data und Recht – Einführung für die Praxis«

C.H. Beck Verlag

1.Auflage 2019 / 184 Seiten
C.H.BECK ISBN 978-3-406-73284-3
65,00 Euro

Die beiden Autoren sind als Berater zur praktischen Umsetzung der datenschutzrechtlichen Anforderungen in einer überregionalen Kanzlei bzw. in einem weltweit agierenden Konzern bekannt. Dementsprechend praxisnah ist ihr Ansatz, komplexe Sachverhalte und noch komplexere rechtliche Anforderungen anschaulich erklären zu müssen. Das Werk richtet sich damit an alle, die sich mit der schwierigen Materie der technischen Möglichkeiten der Verarbeitung von Daten befassen und dies anschaulich begreifen oder erklären müssen, welche Abhängigkeiten und Voraussetzungen aus rechtlicher Sicht zu beachten sind.

Das Werk ist klar gegliedert in 16 Kapitel, in denen die Grundlagen wie personenbezogene Daten, Verantwortlichkeiten und Anforderungen an die Fachkunde des betreuenden Datenschutzbeauftragten vorangestellt werden. Danach folgen die Ausführungen zu den rechtlichen Grundlagen einschließlich der Besonderheiten bei Drittstaatentransfer und Details wie Löschpflichten und relevante Betroffenenrechte. Erläuterungen zur Datenschutz-Folgenabschätzung, zu Schutzmaßnahmen (einschließlich der Behandlung des Urheberrechtsschutzes bei Algorithmen) und zu den Rechtsfolgen der Missachtung rechtlicher Anforderungen runden die Erläuterungen ab.

Abschließend ergänzen zusammenfassende Darstellungen zu Sanktionen wegen Verrats von Betriebs- und Geschäftsgeheimnissen und zu Big-Data-Anwendungen als Service das Werk ab. Hervorzuheben sind hierbei die insgesamt 74 anschaulichen graphischen Abbildungen, welche das Verständnis der komplexen Fragestellungen und Anforderungen erheblich erleichtern. Das Werk schließt mit 10 Handlungsempfehlungen für das Big Data Geschäft.

In den einzelnen Kapiteln werden die jeweiligen Erläuterungen durch Leitsätze abgeschlossen, in welchen die Kernaussagen der vorherigen Ausführungen kurz und bündig zusammengefasst werden.

Für die Abbildungen zur Veranschaulichung komplizier Abläufe und Abhängigkeiten werden neu geschaffene Icons verwendet, die zu Beginn des Werkes erklärt werden. Auch wenn die Verwendung des nach dem BDSG a.F. eingeführten Begriffs der „Vorabkontrolle“ in diesem Werk in einem anderen Zusammenhang verwendet wird: Man erkennt schnell, dass in diesem Kontext die Überprüfung der angemessenen Einhaltung der datenschutzrechtlichen Anforderungen gemeint ist.

Hervorzuheben ist die erkennbare Praxisnähe, die sich nicht auf die Darstellung der ungeheuer vielen Möglichkeiten der Big Data-Verarbeitungen konzentriert, sondern die vielfältigen Anforderungen wie die urheberrechtlichen Aspekte von Datenbanken, Möglichkeiten der Anonymisierung, Vermengung von Datenquellen und auch die für Verantwortliche unbequemen Aussagen zu den Qualifikationsanforderungen des beratenden Datenschutzbeauftragten anschaulich und verständlich behandelt.

Für alle, die sich mit der rechtlichen Zulässigkeit und den Gestaltungsmöglichkeiten der Verarbeitung von personenbezogenen Daten, aber auch von nicht personenbezogenen Daten befassen wollen oder müssen, liegt mit diesem Buch ein sehr empfehlenswertes Werk vor, das auch in Einzelfragen aufgrund der guten Gliederung schnell Erläuterung und Hilfestellung bietet.

„DAS NEUE DATENSCHUTZRECHT IN DER BETRIEBLICHEN PRAXIS“

Laue / Kremer

Laue / Kremer
»Das neue Datenschutzrecht in der betrieblichen Praxis«

Nomos Verlagsgesellschaft Baden-Baden

2. Auflage 2019 / 398 Seiten
ISBN 978-8487-4392-6
48,00 Euro

Im Vergleich zur ersten Auflage ist Dr. Judith Nink aus dem Autorenteam ausgeschieden und die zweite Auflage wird von den übrigen Autoren Dr. Philipp Laue und Sascha Kremer fortgeführt. Die Zielsetzung des Werkes bleibt unverändert: Eine kompakte Aufbereitung der Datenschutz-Grundverordnung, die dem Rechtsanwender in der betrieblichen Praxis konkrete Lösungsvorschläge an die Hand gibt und Orientierung bietet.

Das Werk gliedert sich in 11 Kapitel, die ihrerseits noch unterteilt werden. Nach der Einführung, innerhalb derer der Anwendungsbereich, die Öffnungsklauseln und die Verarbeitungsgrundsätze dargestellt werden, schließen sich die Ausführungen zur Zulässigkeit der Verarbeitung einschließlich der besonderen Kategorien sowie u.a. zum Medienprivileg an. Nach den Informationspflichten und den weiteren Rechten der Betroffenen folgt jeweils ein eigenes Kapitel für die Auftragsverarbeitung und zum Datenschutzbeauftragten. Ebenso erhalten die Erörterungen zu den technischen und organisatorischen Maßnahmen ein eigenes Kapitel, wie die Selbstregulierung mit Verhaltensregeln und Zertifizierung. Mit Erläuterungen zum Beschäftigtendatenschutz, zu der Zusammenarbeit mit Aufsichtsbehörden und zur Haftung werden alle wesentlichen Themen im betrieblichen Alltag umfasst. Auch wenn Webseiten und die damit verbundenen Fragestellungen wie zum Einsatz von Cookies kein eigenes Kapitel erhalten haben, werden bei der Einwilligung doch auch ausreichende Hinweise ausgeführt.

Durch die klare Gliederung und die Unterpunkte in den Kapiteln eignet sich das Handbuch nicht nur als umfassende Einstiegshilfe in die komplexe Rechtsmaterie, sondern bietet auch bei gezielter Suche gut auffindbare Themengebiete.

Bei einigen Darstellungen werden zur Verdeutlichung Tabellen mit Übersichten herangezogen, um übersichtlich beispielsweise die Umsetzung bei den Öffnungsklauseln oder Veränderungen zum bisherigen Recht wie bei den Informationspflichten zu verdeutlichen. Auch wenn sich die Autoren nur zum Ziel gesetzt haben eine praxisnahe Unterstützung zu schaffen, gehen sie an vielen Stellen auch auf die noch nicht abgeschlossenen Diskussionen ein, wie zum Unternehmensbegriff im Rahmen des Kapitels zur Haftung und zu den Sanktionen.

Ein insgesamt empfehlenswertes Werk, das einen guten Überblick zu den relevanten Fragestellungen eines Unternehmens bietet.

Rezensionen von

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

DIGITALISIERTE VERWALTUNG – VERNETZTES E-GOVERNMENT

Margrit Seckelmann (Hrsg.)

Margrit Seckelmann (Hrsg.)
»Digitalisierte Verwaltung – Vernetztes E-Government«

Erich Schmidt Verlag

2. Auflage
2019 / 756 Seiten
94,00 Euro

Für Datenschutzbeauftragte von Behörden relevante Informationen bietet das von Margrit Seckelmann herausgegebene Werk „Digitalisierte Verwaltung - Vernetztes E-Government“. Als Handbuch soll es theoretische wie praktische Antworten geben. Auch wenn Datenschutz nur ein Nebenthema ist, hilft es Datenschutzbeauftragten gerade mit relevanten rechtlichen Hintergründen weiter. In der öffentlichen Verwaltung spielen die vielfältigen Regulierungen eine (noch erheblich) größere Rolle als im privatwirtschaftlichen Bereich. Die Grundlagen des Datenschutzes im öffentlichen Bereich muss man als Grundlage zwar bereits verstanden haben, das Buch beinhaltet aber viele Rechtsthemen, die in dem Bereich der Digitalisierung der Verwaltung relevant sind.

Der Band widmet sich den folgenden Fragen: Was sind die Ziele von E-Government, Open Government und der Digitalisierung? Wie sieht der Regelungsrahmen aus? Welche Aspekte sind bei der Digitalisierung von Verwaltungsverfahren relevant? Wie sieht digitale Kommunikation und digitale Aktenführung für eine Behörde aus? Mit diesen Fragen aus einer sinnvollen Verwaltungssicht holt das Buch sicherlich viele Leser mit Verwaltungshintergrund ab. In das Thema Datenschutz wird ebenso eingeführt. Es werden weitere Einzelthemen, Einsatzgebiete und Detaillösungen behandelt.

Bei der Beurteilung des Bandes ist zu berücksichtigen, dass die Aufarbeitung des Themas insgesamt eines sehr beachtlichen Spagats bedarf. Die E-Government-Regulierung beginnt auf der einen Seite abstrakt auf europäischer Ebene, betrachtet die nationale und dann die für die meisten behördlichen Datenschutzbeauftragten relevante rechtliche Ebene des jeweiligen Bundeslandes und prallt auf der anderen Seite auf technische und praktische Probleme der Umsetzung und die Verwaltungshistorie, die im Kontrast steht zu den technischen Möglichkeiten. Die Stärke des Werks liegt sicherlich eher auf der rechtlichen und theoretischen Seite. Wer sich auf der praktischen Ebene der digitalisierten Verwaltung praktische und rechtliche Lösungen erhofft, wird in diesem Band allerdings nur in wenigen Spezialfragen fündig. Insgesamt geht es eher um Verankerungen für die eigene detaillierte Beschäftigung mit den Rechtsthemen. Das ist durchaus sachgerecht, auch wenn das nicht dem Charakter eines Handbuchs entspricht. Denn in vielen Bereichen muss der aktuelle Stand eines Weges beleuchtet werden, der sich noch kontinuierlich im dynamischen Fluss befindet. Heutige Antworten sehen im Konkreten naturgemäß anders aus als die Ergebnisse in der nahen Zukunft.

Eine weitere Herausforderung ergibt sich auch aus der föderalen Perspektive. Es ist für ein solches Werk praktisch kaum zu behandeln, wie die unterschiedliche Landesgesetzgebung aussieht und welche Unterschiede dort jeweils zu finden sind. Dennoch hätte man sich in dem Werk dazu wesentlich mehr Hinweise gewünscht, die es ermöglichen zumindest den Stand der eigenen Regelungen besser erarbeitbar zu machen. An vielen Stellen bleibt es aber bei der Behandlung der jeweiligen Bundesregelungen ohne ausreichende Hinweise auf die jeweilige relevante Landesgesetzgebung. Bei der Beurteilung dieses Umstands sollte klar sein, dass der Umfang der Verwaltungsbereiche in denen die Landesgesetzgebung anzuwenden ist (kommunale Ebene bis zur Landesebene), den Umfang der Bereiche für die ausschließlich Bundesgesetzgebung anzuwenden ist, deutlich übersteigt.

Zur Anwendung der Inhalte muss also ein Leser bereits einiges an Kenntnissen mitbringen. Derjenige, der sich das Werk erarbeitet, findet aber eine Vielzahl relevanter Detail- und Sachfragen, die in naher Zukunft weiterer Klärung bedürfen. Der Band schärft den Blick auf die unterschiedlichen rechtlichen Fragestellungen und hilft für die konstruktive Auseinandersetzung mit den relevanten Themen. Datenschutzbeauftragte erhalten die nötigen Anhaltspunkte für die Komplexität und den Umfang der zu digitalisierenden öffentlichen Aufgaben, zu denen sie fachkundig die Einhaltung der datenschutzrechtlichen Anforderungen beraten sollen.

Rezensionen von

Dr. Kai-Uwe Loser
Diplom Informatiker, Datenschutzauditor
Datenschutzbeauftragter der Ruhr-Universität Bochum
und der Universität Duisburg-Essen.
Vorstandsmitglied BvD e.V.

REZENSIONEN

DATENSCHUTZ IM KRANKENHAUS – MIT ALLEN NEUERUNGEN DURCH DIE DS-GVO

Andrea Hauser/Ina Haag

Andrea Hauser/Ina Haag
»Datenschutz im Krankenhaus – mit allen Neuerungen durch die DS-GVO«

Deutsche Krankenhaus
Verlagsgesellschaft mbH

Andrea Hauser/Ina Haag
Düsseldorf. 5. Aufl. 2019
ISBN 978-3-942734-25-7
45,00 Euro

Gesundheitsdatenschutz gehört allein schon auf Grund der auf die verschiedensten Gesetze und Verordnungen wie DS-GVO, BDSG, LDSG, SGB, AMG, RöV, KHG, DSG, GDSG usw. verteilten rechtlichen Rahmenbedingungen zu den unüberschaubarsten Rechtsgebieten. Zudem erfolgt durch die Datenschutz-Aufsichtsbehörden noch eine uneinheitliche Auslegung der zahlreichen gesetzlichen Regelungen, so dass selbst in Deutschland von einem Bundesland zum anderen eine einheitliche Auslegung kaum möglich erscheint. Dementsprechend existieren nur wenige Werke, die sich dieser Thematik annehmen.

Das 2012 zuletzt überarbeitete Buch wurde von den Autorinnen anlässlich des Wirkeintritts der DS-GVO überarbeitet. Das Buch soll entsprechend des Vorwortes „einen umfassenden Überblick über sämtliche relevanten Fragestellungen zum Thema Datenschutz im Krankenhaus geben". Dies gelingt den Autorinnen nur eingeschränkt, da sich das Werk auf die Verarbeitung von Patientendaten fokussiert. Andere im Krankenhaus vorhandene datenschutzrechtliche Fragestellungen, wie zum Beispiel Beschäftigtendatenschutz oder Datenschutz bei der medizinischen Forschung, werden nicht bzw. nur am Rande besprochen. Hier wäre ein entsprechender Hinweis im Vorwort oder eine Anpassung des Titels wünschenswert, damit Missverständnisse von Anfang an ausgeschlossen werden.

Das Buch richtet sich weniger an Juristen, die eine Kommentierung zu den verschiedenen Gesetzestexten suchen, sondern an die praxisorientierten Rechtsanwender. So schreiben die Autorinnen beispielsweise, dass die deutschen Kirchen-Datenschutzgesetze gegenüber der DS-GVO Anwendungsvorrang haben; eine Aussage, welche den im Europarecht bewanderten Juristen aufgrund Art. 288 Abs. 2 AEUV wie auch der aktuellen Rechtsprechung des EuGH im Bereich Anwendbarkeit des kirchlichen Arbeitsrecht mit Verwunderung erfüllen wird. Betrachtet man die Fragestellung hingegen aus Sicht des Rechtsanwenders, so stimmt die Aussage in der Praxis: Solange gegen das Recht nicht geklagt wird und der EuGH anders entscheidet, ist das Recht anzuwenden. Da nicht anzunehmen ist, dass eine kirchliche Datenschutzaufsichtsbehörde oder ein kirchliches Krankenhaus gegen die eigene deutsche Kirche den Klageweg beschreitet, ist das Recht dementsprechend anzuwenden. Diese Praxisnähe ist von den Autorinnen gewollt. Wie die Autorinnen selbst schreiben, soll das Buch „eine nützliche Arbeitshilfe in der täglichen Krankenhauspraxis" darstellen. Diesem Anspruch, dem die Autorinnen im Großen und Ganzen gut nachkommen, wird von einer Mehrheit der Leser sicherlich begrüßt.

In einer kurzen Einführung gehen die Autorinnen zunächst auf das Recht auf informationelle Selbstbestimmung wie auch bzgl. der Hintergründe und Ziele der DS-GVO ein, um dann die Bedeutung des Patientendatenschutzes darzustellen. Die übersichtliche Darstellung der verschiedenen Normen, die es zu beachten gibt, wird nicht nur von neuen Datenschutzbeauftragten dankbar entgegengenommen werden.

Wünschenswert wäre hier ein kurzer Abschnitt gewesen, welchen Vorgaben der DS-GVO ein Bundes- oder Landesrecht genügen muss, um anwendbar zu sein. Viele Landeskrankenhausgesetze sind schon mehrere Jahre alt und ob dort verankerten Erlaubnistatbestände den Anforderungen der DS-GVO genügen und somit eine landesspezifische Anwendung einer oder mehrerer Öffnungsklauseln der DS-GVO entsprechen, sollte der Rechtsanwender beachten – gerade in Anbetracht der deutlich erhöhten Bußgelder wie auch der ausgeweiteten Bußgeldtatbestände einerseits und der Ankündigung der deutschen Datenschutz-Aufsichtsbehörden den im Europarecht verankerten Anwendungsvorrang der DS-GVO anzuwenden.

Es fällt auf, dass die vom europäischen Datenschuss-Ausschuss angenommenen Ausarbeitungen der Artikel-29-Datenschutzgruppe nicht immer hinreichend gewürdigt werden, z.B. bei der Betrachtung der von den Autorinnen dargestellten Umgang mit den Betroffenenrechte, insbesondere dem Recht auf Datenübertragbarkeit. Da der europäische Datenschutz-Ausschuss Vorgaben für die einheitliche Auslegung der DS-GVO in Europa geben kann, kommt diesen Ausarbeitungen natürlich eine besondere Bedeutung zu. Gerade, wenn die Autorinnen hier abweichende Meinungen vertreten, wäre auf Grund der oben dargestellten Bußgeldtatbestände eine entsprechende Information des Lesers wünschenswert.

Die Autorinnen führen des Öfteren schon ältere Gerichtsurteile an, bei denen die dem Urteilsspruch zugrundeliegenden Gesetze nicht mehr oder nicht mehr in der dem Urteil zugrundeliegenden Form existieren. Dies ist z.B. bei der Betrachtung der aus § 203 StGB resultierenden beruflichen Schweigepflicht der Fall, wenn Urteile bzgl. des Begriffs „ärztliche Gehilfe" herangezogen werden. Der Begriff des „berufsmäßig tätigen Gehilfen" findet sich auch im aktuellen Gesetz, aber neben diesem Gehilfenbegriff gibt es noch andere Mitwirkende wie zur Vorbereitung „auf den Beruf tätigen Personen" und „sonstige Personen", und in der Gesetzesbegründung findet sich eine Darstellung, wer in Abgrenzung zum „berufsmäßig tätigen Gehilfen" zu den sonstigen Personen zählt. Hier wäre eine Betrachtung, inwieweit die von den Autorinnen angeführten Urteile unter der geänderten Rechtslage noch gültig sind, wünschenswert.

Bei aller Kritik ist das vorliegende Werk eines der wenigen, welches sich an einer umfassenden Darstellung der datenschutzrechtlichen Anforderung bei der Verarbeitung von Patientendaten im Krankenhaus versucht. Dem Berufseinsteiger wird der Einstieg allein schon durch die Darstellung vorhandener Normen ungemein erleichtert. Die vielen Fallbeispiele bieten auch erfahrenen Datenschutzbeauftragten einen schnellen Einblick in verschiedene Themenbereiche wie beispielsweise den Einsatz von Medizinprodukteberatern im OP oder den Umgang mit Patientenarmbändern. Die Nutzung des Buches ermöglicht schnell und unkompliziert die Einholung einer Zweitmeinung, so dass das Buch durchaus eine Empfehlung verdient. Allerdings sollte das Werk nicht als einzige Quelle hinsichtlich der Interpretation der rechtlichen Rahmenbedingungen genutzt werden.

Rezension von

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

ARBEITSRECHT 4.0

Arnold/Günther

Arnold/Günther
»Arbeitsrecht 4.0«
Praxishandbuch zum Arbeits-, IP- und Datenschutzrecht in einer digitalisierten Arbeitswelt

C.H. Beck Verlag

2018, 298 Seiten
ISBN 978-3-406-72213-4
59,00 Euro

Um was geht es? Es geht um Schlagwörter wie „Arbeit 4.0“, „Industrie 4.0“, um die „Vierte industrielle Revolution“. All diese Schlagwörter beschäftigen die Gesellschaft, den Gesetzgeber, die Industrie und den Datenschutzbeauftragten. Der Zusatz „4.0“ soll den technischen Quantensprung verdeutlichen.

Das Buch besteht aus sieben Kapitel und jedes Kapitel i.d.R. aus drei bis fünf Unterkapitel. Es verfügt über ein sehr umfassendes Literaturverzeichnis. Das Buch beleuchtet (Inhaltsübersicht):

- Kap. 1: Digitalisierung und Industrie 4.0
- Kap. 2: Neue/Alternative Beschäftigungsformen
- Kap. 3: Flexibilisierung im individuellen Arbeitsrecht
- Kap. 4: Arbeits- und Gesundheitsschutz/Haftung im Arbeitsverhältnis
- Kap. 5: Geistiges Eigentum und Wettbewerbsrecht im Arbeitsverhältnis
- Kap. 6: Datenschutzrecht (Datenschutz beim Einsatz neuer Technologien m Bewerbungsverfahren, Big Data und People Analytics, Datenschutz in der Smart Factory, Social Media als Mittel der unternehmensinternen Kommunikation, Social Media Plattformen im Konzern, Datenschutzrechtliche Rahmenbedingungen für die Nutzung von Cloud Computing)
- Kap. 7: Kollektives Arbeitsrecht 4.0

Diese Struktur erleichtert ein einfaches Nachschlagen und es ist weder erforderlich die Kapitel noch das Buch im Ganzen zu lesen. Der Leser kann sich seinen Begriff, sein Thema, sein Kapitel suchen ohne gleich verloren in Begrifflichkeiten oder Zusammenhängen zu sein. Dies macht das Arbeiten mit dem Buch sehr angenehm.

Es ist ein Buch für Praktiker. Es wird nicht theoretisiert, es wird vor allem weitergedacht, analysiert und es werden klare Handlungsempfehlungen gegeben.

Das Handbuch bietet einen umfassenden Überblick darüber, welche rechtlichen Themen sich in der Arbeitswelt 4.0 stellen und bietet Vorschläge für (mögliche) Lösungen sowie die Darstellung aller arbeitsrechtlichen Aspekte der digitalisierten Arbeit. Es werden grundsätzliche Fragen, Risiken und Chancen der Digitalisierung aufgezeigt - verbunden mit Lösungsvorschlägen aus der Beraterpraxis.

Höchst lesenswert und empfehlenswert gehört es in das Bücherregal eines jeden, der sich beruflich mit einer digitalisierten Arbeitswelt auseinandersetzt.

DATENSCHUTZ NACH DER EU-DATEN-SCHUTZ-GRUNDVERORDNUNG

Jochen Schneider (BDSG 2018)

Jochen Schneider (BDSG 2018)
»Datenschutz nach der EU-Datenschutz-Grundverordnung«

C.H. Beck Verlag

2. Auflage 2019/ 372 Seiten – broschiert
ISBN 978-3-406-72861-7
29,80 Euro

Prof. Dr. Jochen Schneider, ist Rechtsanwalt (Datenschutzrecht für Unternehmen und Behörden, IT-Recht für Unternehmen und Behörden) in München sowie Honorarprofessor an der LMU. Er zählt zu den Großen des EDV-Rechts und ist seit vielen Jahren ein Kenner des Datenschutzrechtsrechts.

Die 2. Auflage beschäftigt sich u. a. auch mit den praktischen Konsequenzen des BDSG. Einige Themen wurden überarbeitet, wie z.B. die Auftragsverarbeitung.

Das Buch ist in 13 Kapitel gegliedert, wendet sich an nicht-öffentliche Stellen und beleuchtet vor allem die betrieblichen Datenschutzkonzepte. Im Anhang sind die Kontaktadressen der Aufsichtsbehörden sowie Hinweise zu den Kurzpapieren der DSK und weiterführende Literaturhinweise zu finden. Das ausführliche Sachverzeichnis ermöglicht einen schnellen Zugriff.

Das Buch arbeitet nicht die Artikel und Paragrafen der Datenschutzgesetze ab, sondern geht themenbezogen (z. B. Einwilligungen, Pflichten des Verarbeiters) vor und zitiert, dort wo es notwendig ist, die entsprechenden Normen. Zum besseren Verständnis tragen auch Beispiele und Erläuterungen bei. Zusammenfassungen und ein klares Fazit für jeden einzelnen Bereich finden sich jeweils am Kapitelende.

Fazit: Das Buch ist eine gute Einführung und ein gelungener Leitfaden für den Umgang mit der Datenschutz-Grundverordnung (DS-GVO) sowie dem Bundesdatenschutzgesetz (BDSG). Geeignet für Einsteiger – aber auch für die Experten im Datenschutz.

DATENSCHUTZ-GRUNDVERORDNUNG GENERAL DATA PROTECTION REGULATION

Thomas Müthlein (Hrsg.)

Thomas Müthlein (Hrsg.)
»DATENSCHUTZ-GRUNDVERORDNUNG«
General Data Protection Regulation

DATAKONEXT

3. aktualisierte Auflage 2018
248 Seiten – broschiert – DIN A5
ISBN 978-3-89577-837-7
24,99 Euro

Die Datenschutz-Grundverordnung (DS-GVO) mit ihren 99 Artikeln und 173 Erwägungsgründen ist deutlich umfangreicher als das Bundesdatenschutzgesetz (BDSG). Zahlreiche Übersetzungs- und Redaktionsfehler erschweren die Textarbeit. Ein Blick in die englische Fassung (GDPR), welche verbindlich ist, ist vielfach hilfreich und erforderlich zum Verständnis und der Interpretation.

Die zweisprachige Textausgabe stellt die amtliche Fassung der DS-GVO in der englischen und deutschen Fassung gegenüber und berücksichtigt dabei die beiden gesetzgeberischen Korrekturen.

Zum Verständnis der DS-GVO sind die 173 amtlichen Erwägungsgründe heranzuziehen. Diese wurden den einzelnen Artikeln zur leichteren Handhabung zugeordnet und sind ebenfalls in englischer und deutscher Sprache, am Ende des Buches, gegenübergestellt.

Das Buch ist für den Nutzer nach Registrierung über einen Content-Code auch online zugänglich (pdf zum Download).

Mein Resümee: Eine gute Arbeitshilfe, auch für diejenigen, die über die deutschen Grenzen hinaus tätig sind und auf eine korrekte Anwendung des englischen Fachvokabulars angewiesen sind, eine Art „kleines Wörterbuch".

Eine übersichtliche, kompakte und hilfreiche zweisprachige Textausgabe für den Praktiker.

Rezensionen von

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

▶ www.AdOrgaSolutions.de

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

Die wichtigsten Daten der BvD-Gremien

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

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

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

04.04.2019	RG Mitte	**07.06.2019**	AK Externe
04.04.2019	AK FinanzDL	**28.06.2019**	RG Nürnberg
10.04.2019	AK Sozial	**28.06.2019**	RG Ulm
11.04.2019	AK Krypto	**18.07.2019**	RG Karlsruhe
12.04.2019	RG Karlsruhe	**17.09.2019**	RG Ost
12./13.04.2019	AK Externe	**27./28.09.2019**	AK Externe
17.05.2019	RG Stuttgart	**11.10.2019**	RG Stuttgart
03.06.2019	RG Ost	**17.10.2019**	AK Sozial
04.06.2019	AK Medizin	**18.10.2019**	RG Nürnberg

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

Termine und Anmeldung finden Sie auf unserer Webseite:
▶ www.bvdnet.de

VERNETZEN SIE SICH MIT UNS:

▶ www.bvdnet.de
XING: https://www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands
TWITTER: www.twitter.com/bvd_datenschutz
BLOG: www.bvdnet.de/themen/bvd-blog/
RSS-Feed: https://www.bvdnet.de/feed/

BVD-STELLENBÖRSE

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

Sie zertifizierte Datenschutzbeauftragte für eine Festanstellung oder als externe Berater. Zur Stellenbörse:
▶ https://www.bvdnet.de/bvd-stellenboerse/

WICHTIGE KONTAKTE

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

Erfahren Sie mehr darüber und fordern Sie Informationen in der Geschäftsstelle unter bvd-gs@bvdnet.de an.

Software

Es gibt Dinge, die gehen niemanden etwas an.

FOLDERFLEX GERMAN STANDARD

Mehr Sicherheit für Ihre vertraulichen Daten.

www.folderflex.de

Marketing

FÜR DEN BESTEN EINDRUCK

www.tpdigitaldruck.de

Trend Point Marketing GmbH

Breitenbachstraße 24-29 | 13509 Berlin

Datenschutz

Die Seminare der udis: Alles, was man zum Thema Datenschutz wissen muss.

Jetzt informieren unter www.udis.de

udis-zertifizierte Datenschutz-Fachkraft udis zert 12345678 www.udis.de

Datenschutz geht zur Schule BvD e.V. DATENSCHUTZ GESTALTEN

Datenschutz geht zur Schule – DSgzS
Eine Initiative des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31 · 10787 Berlin
Telefon (030) 26 36 77 62 · Telefax (030) 26 36 77 63
dsgzs@bvdnet.de · www.bvdnet.de/dsgzs

Hier könnte Ihre Anzeige stehen!

Jetzt Infos anfordern unter:

bvd-gs@bvdnet.de

Wettbewerb

Verleihung Datenschutz Medienpreis des BvD (DAME)

DAME 2018 BvD-DATENSCHUTZ MEDIENPREIS

Auditierung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH

EIN UNTERNEHMEN VON GDD UND BVD

Datenschutz Zertifizierung:
unabhängig – transparent – standard-basiert

www.dsz-audit.de

Anzeige

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

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

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

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

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

Datenschutz im Fokus.

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

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

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

Abbestellung bis 6 Wochen vor Jahresende.
Preise inkl. MwSt., zzgl. Vertriebs-/Direktbeorderungsgebühren (€ 14,20/€ 5,–) € 19,20 jährlich.

beck-shop.de/go/ZD

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