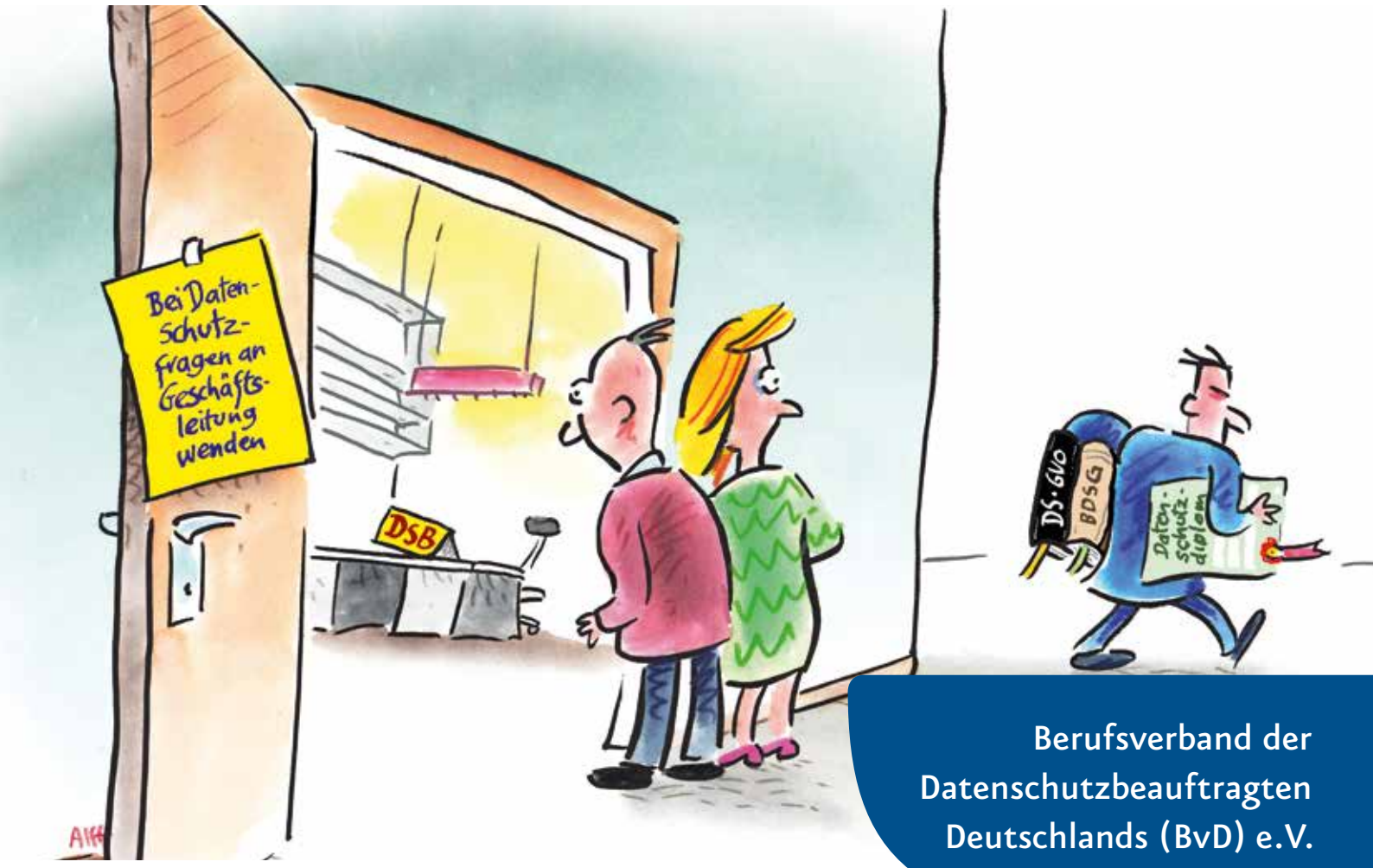
Ausgabe 03/2018

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz



Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Datenschutz – komplex, aber gestaltbar

DAS KOPPLUNGSVERBOT UND DIE DS-GVO – ab S. 16

SECURITY BREACH NOTIFICATION – RISIKEN DER MELDEPFLICHT – ab S. 44

DATENSCHUTZ IN KMU UND VEREINEN – ab S. 64

VOM DATENSCHUTZ ZUR HUMANZENTRIERTEN DATENWIRTSCHAFT – ab S. 71

BvD e.V.
DATENSCHUTZ GESTALTEN

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

BvD e.V.
DATENSCHUTZ GESTALTEN

2019 BvD-Veranstaltungen

Verbandstage 2019
30 Jahre BvD
SONDERSEMINARE AM VORTAG

05. - 06.06.2019
ELLINGTON HOTEL BERLIN

Verleihung
Datenschutz Medienpreis des BvD (DAME)
am 05.06.2019 zur Abendveranstaltung

BvD-Herbstkonferenz zum Datenschutz 2019
WIRTSCHAFT TRIFFT AUFSICHT

23. - 25.10.2019
LE MERIDIEN GRAND HOTEL NÜRNBERG

Das Bayerische Landesamt für Datenschutzaufsicht, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg und der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. laden zum Informationsaustausch ein.

Gemeinsame Veranstaltung von:

BayLDA · Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg · BvD e.V. DATENSCHUTZ GESTALTEN

DEUTSCHLAND UND DIE DS-GVO

Liebe Leserinnen und Leser,

nach dem unterirdischen Presseecho, vielen Scherzen auf Kosten der DS-GVO und auch unglaublichen Auslegungsversuchen gehen die meisten Unternehmen zur Tagesordnung über und packen die Umsetzung einfach an. Dabei kann man sicher nicht auf die manchmal abenteuerlichen Deutungen oder die teilweise noch sehr spitzfindigen Auslegungen von Seiten der zahlreichen „neuen Experten" zurückgreifen, sondern muss sich an der Praxis orientieren. Die von Seiten einiger Aufsichtsbehörden herausgestellte Auffassung, *das die Regelungen dem Betroffenen dienen sollen und nicht um ihrer selbst willen zu befolgen sind*, mag dabei als Leitfaden dienen.

Ganz anders sieht das in der Politik aus. Dort scheint das Thema manchen erst in den letzten Wochen erreicht zu haben und mangels Fachkenntnis wird den absurden Berichten und Übertreibungen offenbar geglaubt und dringender Handlungsbedarf vermutet. Der Ruf nach dem Abbau von Bürokratie ist nun gerade von denen zu vernehmen, die von der Praxis in den Unternehmen noch nicht viel gesehen haben. Qualifizierte betriebliche Datenschutzbeauftragte sind eine Institution zur Vermeidung von Bürokratie. Ein fachkundiger Datenschutzbeauftragter wird stets bemüht, sein in den Unternehmen so praxisgerecht und prozessorientiert wie möglich zu beraten – die Betroffenenrechte selbstverständlich stets im Blick. Ein reiner Rechtsberater, der vom Schreibtisch aus tätig wird, kann das nicht leisten – denn es zählt die Nähe zur betrieblichen Praxis.

Überbringer der schlechten Nachricht – die Datenschutzbeauftragten

Leider sind die Regelungen der DS-GVO zu den Aufgaben des betrieblichen und behördlichen Datenschutzbeauftragten dabei nicht immer hilfreich. Während der Datenschutzbeauftragte im alten BDSG noch in vielen Bereichen konkret tätig geworden ist, kann oder muss er nun durch den Verantwortlichen eingebunden oder hinzugezogen werden. Das setzt aber voraus, dass der Verantwortliche weiß, wann genau das der Fall ist und dieses auch sicher umsetzt. Da die meisten Verantwortlichen ihre datenschutzrechtlichen Pflichten gar nicht kennen, gilt der Datenschutzbeauftragte dann schnell als der Überbringer der schlechten Nachricht – nämlich der bis dahin unbekannten Pflichten und Aufgaben des Verantwortlichen. Das ist dann ein wenig so wie die Hand auf der heißen Herdplatte – da fasst man auch nicht mehr hin.

Die Vorteile der Datenschutzbeauftragten im Gesetz verankern!

Die Praxis sieht daher oft anders aus. Als Beispiel mag die Datenschutz-Folgenabschätzung (DSFA) dienen oder auch das Verzeichnis der Verarbeitungstätigkeiten. Natürlich trägt der Verantwortliche die „Verantwortung" für diese Themen, die „Erstellung" der DSFA und das „Führen" der Verarbeitungsübersicht ist aber beim Datenschutzbeauftragten erheblich besser aufgehoben. Dieser hat die Expertise, um die Aufgaben effizient und korrekt durchzuführen, ohne dass endlose „Runden" gedreht werden müssen. Vorausgesetzt der Datenschutzbeauftragte wird rechtzeitig eingebunden und die Fachbereiche arbeiten vernünftig mit. Dies sind die wichtigsten Zutaten für eine erfolgreiche Umsetzung der Anforderungen aus DS-GVO und BDSG. Die Aufsichtsbehörden raten oft sogar dazu, dem Datenschutzbeauftragten die Aufgaben zu übertragen.

Die logische Konsequenz muss doch sein, dieses auch so im Datenschutzrecht zu verankern. Alle wissen, dass die Aufgaben meist nur durch den DSB bearbeitet werden können – also schreiben wir das doch bitte auch so in das Gesetz. Damit vermeiden wir eine Menge betriebliches Hin-und-her und wir nehmen das Damoklesschwert der Haftung vom DSB, wenn er heute Aufgaben des Verantwortlichen wahrnimmt. Hier ist der deutsche Gesetzgeber gefordert, mit der Erfahrung aus über 40 Jahren Datenschutzrecht - Akzente zu setzen und den Datenschutzbeauftragten fest in den betrieblichen Prozessen zu verankern.

Der BvD hat dazu konkrete Vorschläge erarbeitet, die den entsprechenden Institutionen vorliegen.

Ich wünsche Ihnen eine anregende Lektüre.

T. Spaeing

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

Lektorat:
Frank Spaeing

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

Deutschland und die DS-GVO – *Thomas Spaeing* 3

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Bayerische Landesregierung befindet sich im Hinblick auf den beschlossenen „Bayerischen Weg" bei der Umsetzung der Datenschutzgrundverordnung (DS-GVO) auf dem „Holzweg" – *Nicole Schmidt, LL.M.* 5
Der Blick von der Außengrenze – Das Markortprinzip aus der Sicht eines Nicht-EU Landes – *Bruno Baeriswyl, Dr.iur.* 7
Wettbewerbsrechtliche Abmahnungen wegen Verstößen gegen die DS-GVO – *Dr. iur. Tilman M. Dralle* 10
Einwilligung – Allheilmittel oder Holzweg? – *Stefan Staub* 13
Das Kopplungsverbot und die DS-GVO – *Thomas Kahl* 16
Löschung im Lichte der neuen DS-GVO – *Interview mit Gerhard Friederici* 20
Joint Controllership-Vereinbarungen (JC-V) – keine Ausnahme, sondern Regel – *Karsten U. Bartels* 23

DATENSCHUTZPRAXIS

Überwachung – die unbekannte Aufgabe? – *Dr. Niels Lepperhoff* 26
Umgang mit Datenpannen: Erfüllung von Melde- und Benachrichtigungspflichten nach der DS-GVO – *Dr. Henrik Hanßen* 30
Pflicht zur Benennung eines Datenschutzbeauftragten und zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten in der Arztpraxis – *Prof. Dr. Thomas Hoeren* 35
Übergabe der Dokumentation bei Wechsel des Datenschutzbeauftragten im Unternehmen – *Dr. Carlo Piltz* 40
Security Breach Notification – Risiken der Meldepflicht – *Dr. Jens Eckhardt* 44
"Human Firewall"- wie Sie Mitarbeiter gezielt zu CEO-Fraud sensibilisieren – *Stefan Bachmann* 48
Datenschutz zum Anfassen - Wie mit einem „Hackerlabor" technische Risiken verständlich vermittelt werden – *Thomas Floß* 52
Die ePrivacy-Verordnung – eine Verordnung für eine datenschutzgerechte elektronische Kommunikation? – *Prof. Dr. Anne Riechert* 55

AUFSICHTSBEHÖRDE

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Gespräch mit der BvD-News Redaktion – *Andrea Voßhoff im Interview* 58
Wie macht man den Datenschutz unter der DS-GVO besser? – *Dr. Stefan Brink* 60
Datenschutz in KMU und Vereinen – *Thomas Kranig* 64

GESELLSCHAFT

Strukturelle Schwächen des EU Cybersecurity Acts – *Jan-Peter Kleinhans* 68
Vom Datenschutz zur human-zentrierten Datenwirtschaft – *Malte Beyer-Katzenberger* 71

AUS DEM VERBAND

Full House für besseren Datenschutz – *BvD-Herbstkonferenz 2018* 74
Mit Humor für den Datenschutzbeauftragten kämpfen – *Cartoon-Serie* 78
Datenschutz gerappt – *Ein Blick hinter die Kulissen* 79
Dozententag 2018 – *Initiative „Datenschutz geht zur Schule" (DSgzS)* 81

REZENSIONEN

DATENSCHUTZ-GRUNDVERORDNUNG – *Ehmann / Selmayr (Hrsg.)* 83
DS-GVO und ePrivacy auf Websites umsetzen – *Benedikt / Buckel / Mammen* 84
Datenschutz in Bayern – *Wilde / Ehmann / Niese / Knoblauch* 85
Antworten für die Praxis: Datenschutz in der Betriebsratsarbeit – *Torsten Lemke* 86
Leitfaden zur Datenschutz-Grundverordnung Umsetzungshilfen für die Praxis – *Lepperhoff/Müthlein* 87
Datenschutz-Grundverordnung: DS-GVO; VO (EU) 2016/679 – *Peter Gola* 88
BDSG/DS-GVO: Kommentar zu DS-GVO, BDSG und den Datenschutzbestimmungen von TMG und TKG – *Dr. Kai-Uwe Plath (Hrsg.)* 89
Datenschutz im Internet - Rechtshandbuch zu DS-GVO und BDSG – *Dr. habil. Silke Jandt / Dr. Roland Steidle (Hrsg)* 90

TERMINE UND KONTAKTE

Termine der Regionalgruppen und Arbeitskreise des BvD 91
Überblick Seminare und Workshops 2019 92

BAYERISCHE LANDESREGIERUNG BEFINDET SICH IM HINBLICK AUF DEN BESCHLOSSENEN „BAYERISCHEN WEG“ BEI DER UMSETZUNG DER DATENSCHUTZGRUNDVERORDNUNG (DS-GVO) AUF DEM „HOLZWEG“

Nicole Schmidt, LL.M.

Der Ministerrat der Bayerischen Staatsregierung hat am 5. Juni 2018 einen Beschluss über die „bürgernahe und mittelstandsfreundliche“ Anwendung der Regelungen der Datenschutzgrundverordnung (DS-GVO) gefasst. Dabei soll hinsichtlich der gestellten Voraussetzungen mit „Augenmaß“ verfahren werden. Mit diesem Beschluss bezweckt die bayerische Landesregierung die im Zuge der Umsetzung der DS-GVO aufgekommene Aufregung in der Wirtschaft und Bevölkerung einzudämmen. Diese war aufgrund der in der DS-GVO verankerten Kombination scharfer Sanktionen und einer Vielzahl an unbestimmten Rechtsbegriffen, welche aufgrund der fehlenden Rechtsprechung noch nicht „ausgefüllt“ wurden, im Vorfeld aufgekommen. Dies noch verstärkend rieten Anwälte aufgrund eben jener fehlenden Rechtsprechung und dem anwaltlichen Vorsichtsgebot zu tiefgreifenden Maßnahmenkatalogen zur Prävention von Datenschutzverletzungen.

Der Brandlöschungsversuch ist der Bayerischen Landesregierung jedoch misslungen. Es ist nicht Teil der Kompetenz des Ministerrates, über die Umsetzung der DS-GVO zu entscheiden und einen „bayerischen Weg“ einzuschlagen. Der Präsident des Bayerischen Landesamt für Datenschutzaufsicht (BayLDA), Thomas Kranig, äußerte richtigerweise in einem Interview gegenüber der DAZ-online seine Bedenken hinsichtlich der Veröffentlichung des Ministerrates, dass die ▸

DS-GVO als unmittelbar anwendbares europäisches Recht einheitlich vollzogen werden muss, sodass es einen abweichenden ‚bayerischen Weg' bei der Umsetzung der DS-GVO naturgemäß nicht geben kann.

Die Wichtigsten der beschlossenen Leitlinien zur Umsetzung sollen im Folgenden dargestellt und kommentiert werden:

- **Amateursportvereine sowie weitere vom Ehrenamt getragene Vereine sollen keinen Datenschutzbeauftragten bestellen müssen.**

Diese Aussage steht im Widerspruch zu Art. 37 Abs. 4 DS-GVO in Verbindung mit § 38 Abs. 1 BDSG (neu), welche die Ernennung eines Datenschutzbeauftragten im Falle der Beschäftigung von zehn oder mehr Personen mit der automatischen Verarbeitung personenbezogener Daten vorschreiben.

- **Sanktionen sollen generell nur im Notfall verhängt werden, insbesondere jedoch nicht nach einem Erstverstoß – Hinweise und Beratung sollen Vorrang haben.**

Auch hier erscheint besonders fraglich, ob diese Praktik den Anforderungen der DS-GVO, wonach Verstöße „wirksam, verhältnismäßig und abschreckend" erfolgen müssen, gerecht wird. Thomas Kranig stellte klar, dass gegenüber denjenigen Verantwortlichen, die sich nicht hinreichend um den Datenschutz kümmern, auch nach Erstverstößen nach pflichtgemäßem Ermessen Sanktionen verhängt werden müssen. Ein Unterschied, ob es sich um Vereine, kleinere Unternehmen etc. handelt, kann dabei nicht gemacht werden.

- **Die Regierung sieht außerdem vor „mit den Betroffenen weitere Bestimmungen im Datenschutzrecht (zu) identifizieren" die zu hart seien, um diese „mit Augenmaß" auf einen erträglicheren Inhalt zu reduzieren.**

Insbesondere in diesem Punkt ist kein „bayerischer Alleingang" möglich, da die Datenschutzgrundverordnung (DS-GVO) in allen Mitgliedstaaten einheitlich vollzogen werden muss. Eine anwendungsfreundliche Handhabung ist, wenn überhaupt, nur im Einklang mit den Datenschutzaufsichtsbehörden der anderen Mitgliedsstaaten möglich.

Abschließend ist hinsichtlich des Ministerratsbeschlusses Resümee zu ziehen. Die Bemühungen gerade den Mittelstand, der unter dem Umfang des Maßnahmenkataloges am meisten leidet, zu beruhigen ist gewiss aller Ehren wert ist. Die Absicht, durch die lockere Handhabung der DS-GVO die Unternehmen vor den Klagen sogenannter Abmahnanwälte zu schützen und diesen das Handwerk zu legen, ist ebenso ein edles Motiv, geht jedoch in die falsche Richtung, da die Datenschutzaufsichtsbehörde in diesem Falle ihre Kompetenz überschreitet und im Zuge dessen zu keiner Beruhigung der Ungewissheit beiträgt.

Der mit Abstand hilfreichste Punkt im Ministerratsbeschluss ist derjenige, der die Vereine und Mittelständler durch das Anbieten einer Anlaufstelle für Gespräche bei der Umsetzung unterstützt. Insbesondere den kleineren, datenverarbeitenden Vereinen oder Betrieben fehlen in der Regel die Mittel oder die Expertise sich wirksam an die Voraussetzungen der DS-GVO anzupassen.

Nun bleibt abzuwarten, ob überhaupt und wenn ja, welche der Punkte des Ministerratsbeschlusses vom Bayerischen Landesamt für Datenschutzaufsicht für den nicht-öffentlichen Bereich übernommen werden.

Es wird fortan wohl das Beste sein, erste Ergebnisse der Rechtsprechung abzuwarten und zunächst Vorsicht walten zu lassen, auch wenn dies das Ergreifen der ein oder anderen unbequemen Maßnahme bedeutet.

Über die Autorin

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

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

swds
DATENSCHUTZRECHT FÜR UNTERNEHMEN

DER BLICK VON DER AUSSENGRENZE – DAS MARTKORTPRINZIP AUS DER SICHT EINES NICHT-EU LANDES

Bruno Baeriswyl, Dr. iur.

Die Schweiz befindet sich mitten in Europa, ist aber nicht Mitglied der Europäischen Union (EU). Umgeben von EU-Mitgliedstaaten – Frankreich, Italien, Österreich, Deutschland – und einem EWR-Land – Liechtenstein – ist die Schweiz auf vielen Ebenen mit diesen Ländern verbunden. Dass die Schweiz auch im Datenschutzrecht mit den europäischen Nachbarn mithalten kann, hat die EU-Kommission bereits im Jahre 2000 festgestellt, indem sie der Schweiz die Gleichwertigkeit ihres Datenschutzrechts bestätigte[1]. Auch den datenschutzrechtlichen Abkommen des Europarates[2] ist die Schweiz beigetreten. Zudem ist die Schweiz Mitglied des Schengen-Raums und hat den entsprechenden Beschluss[3] in ihr nationales Recht umgesetzt. Sie ist nun auch dabei, die neue Richtlinie[4] in diesem Bereich umzusetzen. Dabei schafft die Schweiz mehrheitlich nicht bereichsspezifisches Datenschutzrecht, sondern setzt die Bestimmungen im allgemeinen Datenschutzrecht des Bundes und der Kantone um.

Irritierendes Marktortprinzip

Mit der DS-GVO hat die EU einen neuen Standard im Bereich des Datenschutzrechts gesetzt. Der Blick von aussen ist nun primär auf die Frage gerichtet, wie es gelingen wird, das Datenschutzrecht innerhalb der EU-Mitgliedstaaten zu vereinheitlichen. Das wird wohl die primäre Aufgabe aller beteiligter Gremien sein, inklusive des Europäischen Gerichtshofs. Aber aus einer Aussensicht stellt sich auch die Frage, wie weit die DS-GVO über die EU hinaus als internationaler Standard Leitbild werden wird. Dabei nimmt sich die DS-GVO schon einmal heraus, über die Grenzen der Mitgliedstaaten hinaus Wirkung zu entfalten. Das Marktortprinzip hält fest, dass nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter unter die DS-GVO fallen, sofern sie Daten von betroffenen Personen, die sich in der Union befinden, in Zusammenhang mit dem Anbieten von Waren und Dienstleistungen (Art. 3 Abs. 2 lit. a DS-GVO) oder deren Verhalten (Art. 3 Abs. 2 lit. b DS-GVO) verarbeiten.

Das wohlgemeinte Ziel dieser Bestimmung, EU Bürgerinnen und Bürgern einen einheitlichen Datenschutzstandard zu bieten, hat aber in erster Linie zu Irritationen geführt. Selbstverständlich erscheint, dass auf Niederlassungen eines Verantwortlichen in der Union die DS-GVO anwendbar ist, aber auch auf Verantwortliche im Ausland in den genannten Fällen? Dabei liefern die Erläuterungen zur DS-GVO einige Erklärungen, aber keine Begründungen zu den grundsätzlichen Fragen. ▸

[1] Entscheid EU Kommission vom 26. Juli 2000 (200/518/EG; Abl. L 215/1 vom 25.8.2000).
[2] Konvention 108 (Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten) (SEV 108); Zusatzprotokoll bezüglich Aufsichtsbehörden und grenzüberschreitender Datenverkehr (SEV 181).
[3] Rahmenbeschluss über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (Rahmenbeschluss 2008/977/JI vom 27. November 2008).

Grundsätzliche Fragen

In erster Linie stellt sich die Frage, wie die Verpflichtungen aus der DS-GVO gegenüber einem Datenverantwortlichen, der seinen Sitz im Ausland hat, überhaupt durchgesetzt werden können. Dazu gehört auch die Verpflichtung, einen Vertreter in der EU zu bestimmen. Grundsätzlich kann eine betroffene Person aber auch in Datenbearbeitungen einwilligen, die von den Prinzipien der DS-GVO abweichen, oder es kann eine andere Rechtswahl getroffen werden, so dass die DS-GVO gar nicht zur Anwendung gelangt. Aus der Sicht der Schweiz wäre aber auch klarzustellen, welches das Verhältnis zwischen dem Angemessenheitsbeschluss und dem Marktortprinzip ist. Macht der Angemessenheitsbeschluss das Marktortprinzip nicht obsolet oder umgekehrt? Auf jeden Fall viele Fragen, die sich aus der Sicht eines Staates stellen, der nicht EU-Mitglied ist, dem aber ein gleichwertiges Datenschutzniveau attestiert wird.

Umgang mit der Rechtsunsicherheit

Diese Ausgangslage hat dem Datenschutz in der Schweiz im Jahre 2018 keine Sternstunde beschieden. Obwohl seit einigen Jahren auch in der Schweiz klar ist, dass das Datenschutzrecht in seiner Wirkung nachgelassen hat und deshalb eine Reform notwendig ist, hat das Inkrafttreten der DS-GVO in der EU nicht zu einer klaren Linie in Bezug auf die Reform des Datenschutzrechts geführt. Im Gegenteil: Die Rechtsunsicherheit in Bezug auf die Geltung der DS-GVO für schweizerische Unternehmen hat zu einer Schwemme von neu berufenen „Datenschutzexperten" geführt, die mit ihren Beratungen und Seminaren den Markt überschwemmen, natürlich mit der unumstösslichen Überzeugung, dass nun die DS-GVO auch für schweizerische Verantwortliche umzusetzen sei und sie einen Vertreter in der EU zu mandatieren hätten.

Entweder geben nun verantwortliche Datenbearbeiter viel Geld aus, um mit der DS-GVO kompatibel zu sein (die schweizerische Wirtschaft ist vielfach mit Kundinnen und Kunden im Ausland verbunden) oder sie machen in Bezug auf den Datenschutz gar nichts: Denn seit einiger Zeit hat man ihnen gesagt, dass das schweizerische Datenschutzrecht reformiert werde und nun soll aber die DS-GVO gelten.

Der Gesetzgeber ist paralysiert

In dieser Situation hat auch der Gesetzgeber die Orientierung verloren. Das von der Regierung vorgelegte Reformprojekt stockt im nationalen Parlament. Wäre eigentlich die Richtung der Datenschutzreform vorgegeben gewesen – die Stärkung der Wirkung des Datenschutzrechts – stehen nun ganz andere Aspekte im Vordergrund: Was muss gemacht werden, um den Angemessenheitsbeschluss der EU zu erhalten? Gilt mit dem Markortprinzip die DS-GVO nicht bereits da, wo sie sollte? Brauchen wir überhaupt eine Reform? Und nicht zuletzt: Es soll auch ein Marktortprinzip in Bezug auf das schweizerische Datenschutzrecht eingeführt werden: Mit anderen Worten: Wer Bürgerinnen und Bürgern in der Schweiz Waren und Dienstleistungen anbietet, hat sich nach dem schweizerischen Datenschutzrecht zu richten! Zusätzlicher Aufwand für Verantwortliche Datenbearbeiter in der EU oder einfach ein Zeichen, das auf die Absurdität der Bestimmung verweist bei einer Ausgangslage, in der beide Seiten sich einen gleichwertigen Datenschutz attestieren?

Diese Situation gibt natürlich nationalistischen Strömungen – auch in der Schweiz – Aufschub. So hat sich das Parlament in der Zwischenzeit auf die Umsetzung der „zwingenden" Bestimmungen der EU aus dem Schengenbereich geeinigt und ein Schengendatenschutzgesetz (SDSG) geschaffen[5]. In Bezug auf die eigentliche Reform des schweizerischen Datenschutzrechts herrscht aber aufgrund der geschilderten Situation keine Einigkeit. Ein allgemeines revidiertes Datenschutzgesetz soll folgen, welches das SDSG wieder ausser Kraft setzt. Aber die Reform wird auch grundsätzlich in Frage gestellt. Dabei verwundert auch nicht, dass die Kantone in ihren Reformprojekten äusserst langsam vorgehen und die zweijährige Umsetzungsfrist in Bezug auf die Bestimmungen aus dem Schengenrecht gelassen vorbeiziehen lassen. In der Schweiz scheint die DS-GVO mit ihrem Marktortprinzip gerade das Gegenteil einer Stärkung des Datenschutzes zu erwirken.

[5] https://www.admin.ch/opc/de/federal-gazette/2018/6003.pdf

Pragmatisches Vorgehen ….

Die Datenschutzaufsichtsbehörden in der Schweiz haben in dieser Situation bisher den kühlen Kopf bewahrt. Sie machen auf die offenen Fragen aufmerksam, ohne verantwortliche Datenbearbeiter zur Anpassung ihrer Datenbearbeitungen an die DS-GVO zu drängen[6]. Das ist auch pragmatisch, bestehen doch noch viele Lücken bei der Umsetzung des geltendem Datenschutzrechts in der Schweiz, das vorgängig einzuhalten wäre. Die Datenschutzaufsichtsbehörden stehen dabei stark im Gegenwind der erwähnten „Datenschutzexperten". Und den Kolleginnen und Kollegen in den EU-Mitgliedländern müssen sie leider mitteilen, dass sie keine Kompetenzen in Bezug auf den Vollzug der DS-GVO in der Schweiz haben!

… und offene Fragen

Damit verbleibt die Beantwortung der offenen Fragen, die sich aus Sicht eines Nicht-EU-Mitgliedstaates stellen.

In erster Linie ist das Marktortprinzip aus völkerrechtlicher Sicht zu betrachten. Wie weit kann ein Staat oder Staatenbund einem Rechtssubjekt in einem anderen Staat unilateral verbindliche Vorgaben machen? Ist das Anbieten von Waren und Dienstleistungen über die Grenzen hinweg in einer globalen Marktwirtschaft nicht selbstverständlich? Sollten rechtliche Defizite bestehen, wäre diesen nicht mit internationalen Abkommen zu begegnen? Hier wäre auch der internationale Vollzug solcher Bestimmungen zu regeln.

Mit den Bestimmungen zur Beurteilung der Angemessenheit des Datenschutzniveaus in einem Land besteht ein Instrument im Bereich des Datenschutzes, das die Autonomie des jeweiligen Staates nicht verletzt. Welche Rolle kann dabei das Marktortprinzip spielen, wenn beide Länder sich gegenseitig einen angemessenen Datenschutz attestieren? Beide Staaten könnten ein Marktortprinzip statuieren, was für die verantwortlichen Datenbearbeiter ausser einem bürokratischen Aufwand keinen Nutzen bringt.

Letztendlich geht es aber um die betroffenen Personen. An ihre Einwilligungserklärungen werden hohe formelle Anforderungen gestellt. Aber materiell können sie umfassend auf ihre Datenschutzrechte verzichten. Dies zeigen die neu formulierten Datenschutzerklärungen der globalen Unternehmen eindrücklich. Nach Inkrafttreten der DS-GVO schreibt Google: „Diesen Monat aktualisieren wir unsere Datenschutzerklärung, (…) „ und „es änderst sich nichts (…) daran, wie Ihre Daten verarbeitet werden".

Dies zeigt deutlich, dass eine Stärkung des Datenschutzes wohl nicht über Bestimmungen wie das Markortprinzip zu erreichen ist.

Fazit

Das Marktortprinzip hat in der Schweiz als Nicht-EU-Mitgliedstaat zu einer grossen Verunsicherung geführt. Das Feld wurde für Akteure geöffnet, die entweder wirtschaftliche oder politische Interessen im Vordergrund haben. Beide agieren nicht auf dem Hintergrund einer Stärkung des Datenschutzes. Es ist zu hoffen, dass in der EU die Auswirkungen des Marktortprinzips auf die anderen Länder kritisch hinterfragt werden. Dabei sollte nicht der formelle – und bürokratische – Vollzug der DS-GVO im Vordergrund stehen, sondern die Frage, wie können die Rechte der betroffenen Personen wirklich gestärkt werden. Die grosse Lücke besteht bei den Einwilligungserklärungen, die nach wie vor den Verantwortlichen alle Türen öffnen. Google lässt grüssen ….

Über den Autor

Bruno Baeriswyl, Dr. iur.

Datenschutzbeauftragter des Kantons Zürich und Mitglied des Vorstandes der Konferenz der schweizerischen Datenschutzbeauftragten (privatim)

▶ www.datenschutz.ch / www.privatim.ch

[6] https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2018/EU%20DS-GVO.pdf.download.pdf/Die_EU_DS-GVO_und_ihre_Auswirkungen_auf_die_Schweiz_DE_V2.pdf ; https://dsb.zh.ch/internet/datenschutzbeauftragter/de/datenschutz/datenschutz/_jcr_content/contentPar/downloadlist/downloaditems/916_1519056093162.spooler.download.1524038053924.pdf/Auswirkungen-der-EU-Datenschutzerlasse.pdf

WETTBEWERBSRECHTLICHE ABMAHNUNGEN WEGEN VERSTÖSSEN GEGEN DIE DS-GVO

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

I. Einleitung

Die Debatte über die Abmahnfähigkeit von DS-GVO-Verstößen auf Grundlage des Gesetzes gegen den unlauteren Wettbewerb (UWG) hat neuen Zündstoff erhalten. Mit einem Beschluss des Landgerichts Würzburg vom 13. September 2018 (Az. 11 O 1741/18 UWG) liegt nun eine erste gerichtliche Entscheidung zu dieser hoch umstrittenen Frage vor. Darüber hinaus gibt es auch auf legislativer Ebene neue Entwicklungen.

II. Die Entscheidung des Landgerichts Würzburg

In dem einstweiligen Verfügungsverfahren vor dem Würzburger Landgericht (LG) ging es um die Internetseite einer Rechtsanwältin. Das Gericht stellte zunächst fest, dass die lediglich sieben Zeilen umfassende Datenschutzerklärung der Antragsgegnerin den Informationspflichten gemäß Artt. 13, 14 DS-GVO nicht genüge. So fehlten Angaben zum/zur Verantwortlichen, zur Erhebung und Speicherung personenbezogener Daten sowie zu den Zwecken der Datenverarbeitung. Auch Informationen zur Weitergabe personenbezogener Daten an Dritte sowie zur Verwendung von Cookies und Analy-

setools seien nicht vorhanden. Schließlich enthalte die Datenschutzerklärung weder einen Hinweis auf die Betroffenenrechte nach Kapitel III DS-GVO, noch auf die Möglichkeit, Beschwerde bei einer Aufsichtsbehörde einzulegen.

Nach dieser Feststellung kam das LG zum Kern des Verfahrens, nämlich dem vom Antragssteller geltend gemachten wettbewerbsrechtlichen Unterlassungsanspruch. Nach Ansicht des Gerichts handelt es sich bei den DS-GVO-Informationspflichten um Marktverhaltensregeln im Sinne des § 3a UWG, d.h. um Vorschriften, „die auch dazu bestimmt [sind], im Interesse der Marktteilnehmer das Marktverhalten zu regeln". Eine mangelhafte Umsetzung der Informationspflichten könne daher, so das Gericht, von Mitbewerbern wie dem Antragsteller als Wettbewerbsverstoß abgemahnt werden. In seinen insgesamt knappen Ausführungen zur Abmahnfähigkeit von DS-GVO-Verstößen nahm das LG Bezug auf Urteile des OLG Hamburg (Urteil v. 27.06.2013, Az. 3 U 26/12) und des OLG Köln (Urteil v. 11.03.2016, Az. 6 U 121/15) aus der „Vor-DS-GVO-Zeit", in denen Verletzungen von Datenschutzvorschriften – konkret die Pflicht zur Vorhaltung einer Datenschutzerklärung gemäß § 13 Abs. 1 TMG – als Verstoß gegen Marktverhaltensregeln und damit gegen Wettbewerbsrecht gewertet wurden.

III. Bewertung des Urteils und Hintergrund

Das Urteil der Würzburger Richter zeigt, dass Abmahnungen gegen DS-GVO-Verstöße durchaus möglich sind. Ob die Entscheidung damit den „Startschuss für Abmahnanwälte" markiert und eine „DS-GVO-Abmahnwelle" lostritt,[1] bleibt Spekulation. Fest steht, dass andere Gerichte ohne Weiteres zu einer divergierenden Rechtsauffassung gelangen könnten. Denn die Entscheidung des LG lässt eine ernsthafte inhaltliche Auseinandersetzung mit der Frage, ob Mitbewerber befugt sind, Verstöße gegen die DS-GVO als Wettbewerbsverstoß abzumahnen, vollständig vermissen. Eine wie auch immer geartete „faktische Bindungswirkung" kommt dem Beschluss vor diesem Hintergrund nicht zu.

Gegen die Anwendbarkeit des bundesdeutschen UWG neben der europäischen DS-GVO spricht, dass die DS-GVO in Kapitel VIII („Rechtsbehelfe, Haftung und Sanktionen") ein Durchsetzungsregime etabliert, das mit guten Gründen als „abschließend" qualifiziert werden kann und damit eine Sperrwirkung gegenüber den UWG-Regelungen entfaltet.[2] Abgesehen von den betroffenen Personen selbst stellen die nationalen Aufsichtsbehörden nach der Grundkonzeption dieses Regimes die zentralen Akteure der Rechtsdurchsetzung dar. Anderen Personen ist die Durchsetzung der von der DS-GVO geschützten Grundrechte und Grundfreiheiten natürlicher Personen nur in engen Grenzen gestattet.

So können die EU-Mitgliedstaaten gemäß Art. 80 Abs. 2 DS-GVO lediglich vorsehen, dass bestimmte Einrichtungen, Organisationen und Vereinigungen auch „unabhängig von einem Auftrag der betroffenen Person" das Recht auf Beschwerde bei einer Aufsichtsbehörde sowie das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegenüber datenverarbeitenden Unternehmen haben. Die Einrichtungen, Organisationen und Vereinigungen müssen dabei ohne Gewinnerzielungsabsicht handeln, ihre satzungsmäßigen Ziele müssen im öffentlichem Interesse liegen und sie müssen im Bereich des Schutzes der Rechte und Freiheiten von betroffenen Personen in Bezug auf den Schutz ihrer personenbezogenen Daten tätig sein. Wettbewerbern hingegen wird kein entsprechendes Recht zugebilligt. Folglich lautet das ***argumentum a minori ad maius*** hier: Wenn der Verordnungsgeber in Art. 80 DS-GVO schon nur bestimmten Verbänden das Recht zugesteht, Rechte betroffener Personen in Eigeninitiative durchzusetzen, dann kann die DS-GVO zulässigerweise nicht dahingehend ausgelegt werden, ähnliche Rechte auch Mitbewerbern einzuräumen.[3]

Die fehlende Regelung der Rechtsbehelfsmöglichkeiten von Mitbewerbern könnte allerdings auch dahingehend ausgelegt werden, dass die DS-GVO diesbezüglich eben keine abschließende Normierung trifft und insofern Freiräume für (bestehende) mitgliedstaatliche Regelungen eröffnet. Auch aus rechtspolitischer Perspektive könnte dieses Ergebnis sinnhaft sein, wenn man bedenkt, dass die Möglichkeit der Geltendmachung wettbewerbsrechtlicher Ansprüche den Umsetzungsdruck für datenverarbeitende Unternehmen intensiviert und somit ein hohes Datenschutzniveau im Sinne der DS-GVO fördert. Zumindest der baden-württembergische Landesdatenschutzbeauftragte, ▶

[1] Siehe https://www.lto.de/recht/hintergruende/h/DS-GVO-abmahnung-abmahnwelle-datenschutz-wettbewerbsrecht/, abgerufen am 24.10.2018.

[2] So die Datenschutzbeauftragte von Schleswig-Holstein, Marit Hansen, im Interview; https://www.handelsblatt.com/22596802.html, abgerufen am 24.10.2018.

[3] Helmut Köhler, „Die DS-GVO – eine neue Einnahmequelle für gewerbsmäßige Abmahner?", ZD 8/2018, S. 337f.

Dr. Stefan Brink, vertritt die Position, dass die Bestimmungen der DS-GVO Unterlassungsansprüchen nach dem UWG nicht entgegenstehen.[4]

IV. Gesetzesänderungen zur Eindämmung von Abmahnungen

Auch auf legislativer Ebene sind Entwicklungen zu verzeichnen. So brachte der Freistaat Bayern am 6. Juli 2018 einen Antrag zur Anpassung zivilrechtlicher Vorschriften an die DS-GVO in den Bundesrat ein.[5] Der Gesetzesentwurf sieht eine ausdrückliche und generelle Herausnahme des Datenschutzrechts aus dem Anwendungsbereich des UWG vor. So soll durch eine Änderung des § 3a UWG klargestellt werden, dass es sich bei den Vorschriften der DS-GVO sowie deren Durchführungsbestimmungen nicht um Marktverhaltensregeln im Sinne der Vorschrift handele. Diese Gesetzesänderung sei erforderlich, „um die Vorgaben der DS-GVO unionsrechtskonform umzusetzen".[6] Darüber hinaus sieht der Gesetzesentwurf auch eine Änderung des Unterlassungsklagengesetzes (UKlaG) vor, demzufolge Verbraucherschutzverbänden Unterlassungs- und Beseitigungsansprüche dann nicht zustehen sollen, wenn eine Informationserteilung gemäß Artt. 13, 14 DS-GVO nicht den gesetzlichen Anforderungen entspricht. Die Ausschussberatungen zu dem Gesetzesantrag dauern derzeit noch an.

Zusätzlich zur Initiative des Freistaats Bayern hat das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) unlängst den Referentenentwurf eines Gesetzes zur Stärkung des fairen Wettbewerbs vorgelegt.[7] Die vorgeschlagenen Gesetzesänderungen sollen missbräuchliche Abmahnungen eindämmen, z.B. durch höhere Anforderungen an die Befugnis zur Geltendmachung von Ansprüchen, die Verringerung finanzieller Anreize für Abmahnungen sowie vereinfachte Möglichkeiten zur Geltendmachung von Gegenansprüchen. So sieht der Entwurf u. a. konkret vor, dass der Anspruch auf Aufwendungsersatz für Mitbewerber und Wirtschaftsverbände ausgeschlossen ist, wenn die Zuwiderhandlung „angesichts ihrer Art, ihrer Schwere, ihres Ausmaßes und ihrer Folgen die Interessen von Verbrauchern, sonstigen Marktteilnehmern und Mitbewerbern in nur unerheblichem Maße beeinträchtigt". Hierzu führt die Gesetzesbegründung weiter aus, dass „[soweit] die in den Artikeln 13 und 14 der Datenschutz-Grundverordnung enthaltenen Gebote als Marktverhaltensregelungen im Sinne von § 3a UWG bewertet werden, […] eine nur unerhebliche Beeinträchtigung im Einzelfall in Betracht kommen [kann], wenn von den aufgelisteten Anforderungen nur geringfügig abgewichen worden ist".[8] Darüber hinaus wird laut BMJV momentan noch beraten, wie ergänzende Sonderregelungen für die Abmahnung datenschutzrechtlicher Verstöße – insbesondere zum Schutz kleinerer und mittlerer Unternehmen – aufgenommen werden können.

V. Fazit

Die beträchtliche Rechtsunsicherheit hinsichtlich der Abmahnfähigkeit von DS-GVO-Verstößen durch Mitbewerber ist auch nach der Entscheidung des Würzburger Landgerichts unverändert. Letztlich wird erst ein Urteil des Europäischen Gerichtshofs oder eine eindeutige Änderung des UWG die erforderliche Klärung der Rechtslage herbeiführen. Bis dahin gilt: Wer die DS-GVO adäquat umsetzt, für den besteht auch wettbewerbsrechtlich keine offene Flanke.

Über den Autor

Dr. iur. Tilman M. Dralle, LL.M. (Nottingham)
Security Consultant mit Schwerpunkt im Bereich IT-Compliance, Datenschutz und Informationssicherheit bei TÜV Rheinland

TÜVRheinland®
Genau. Richtig.

[4] Siehe <http://blogs.faz.net/einspruch/2018/08/29/das-ganz-grosse-DS-GVO-interview-330/>, abgerufen am 24.10.2018.

[5] Siehe Bundesrats-Drucksache 304/18.

[6] ibid., S. 7.

[7] Siehe <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/St%C3%A4rkung_fairen_Wettbewerbs.html>, abgerufen am 24.10.2018.

[8] ibid., S. 25.

EINWILLIGUNG – ALLHEILMITTEL ODER HOLZWEG?

Michael Schlagintweit

Wer glaubt, die Einwilligung als Rechtsgrundlage für die Verarbeitung sei das „Allheilmittel", ist definitiv auf dem Holzweg.

Derzeit kursieren vielfach E-Mails mit:

- „Wenn Sie nichts unternehmen, sind Sie damit einverstanden."
- „Teilnehmer sind damit einverstanden, dass sie gefilmt werden."

Noch viel häufiger und auch nerviger ist jedoch das Cookie-Banner. Es versperrt einem die Sicht auf die Webseite und bietet meistens nur die Option „Accept". Ein „Nein" steht in der Regel nicht zur Verfügung. Und es wäre auch zwecklos, denn die Cookies wurden beim Einblenden des Cookie-Banners schon längst gesetzt. In vielen Fällen verdeckt das Cookie-Banner auch noch den Link zum Impressum und zur Datenschutzerklärung, d.h. man muss die Cookies akzeptieren, bevor man eine ladungsfähige Anschrift des Verantwortlichen und Informationen zum Datenschutz erhält.

Willkommen in der Anwendung der Datenschutz-Grundverordnung – **so macht man es nicht.**

Deshalb schauen wir zunächst auf die Einwilligung und dann auf die Alternativen.

In der Datenschutz-Grundverordnung (DS-GVO) wird zur Einwilligung folgendes ausgeführt:

- eindeutige Handlung (Art. 4 DS-GVO)
- jederzeit widerrufbar (Art. 7 DS-GVO)

Eine Einwilligung ist also jederzeit widerrufbar.

Ob die Einwilligung eine gute Rechtsgrundlage für die Verarbeitung ist, hängt davon ab, ob der Verantwortliche einen Widerruf der Einwilligung vollumfänglich erfüllen kann.

Für einen E-Mail-Newsletter ist die Einwilligung ein guter und praktikabler Weg. Für eine vertragsrelevante Verarbeitung, in der beispielsweise wegen Aufbewahrungspflichten die Daten nicht gelöscht werden dürfen, ist die Einwilligung ungeeignet. Die Einwilligung ist auch immer dann fehl am Platz, wenn man durch den Widerruf der Einwilligung die Datenverarbeitung einstellen muss, jedoch auf die Daten zwingend angewiesen ist.

Dann ist noch die Frage offen, wie man zu der Einwilligung gekommen ist. Nach Erwägungsgrund (EWG) 32 gilt: „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der ▸

betroffenen Person sollten daher keine Einwilligung darstellen". Eine Einwilligung muss immer bewusst erteilt werden.

Aus diesem Grund sollte man sich die **Alternativen** für eine Rechtsgrundlage ansehen. In Art. 6 Abs. 1 DS-GVO sind folgende Bedingungen für rechtmäßige Datenverarbeitungen aufgeführt (Kurzform):

b) Vertragserfüllung

c) rechtliche Verpflichtung

d) lebenswichtiges Interesse

e) öffentliches Interesse

f) berechtigtes Interesse

(Art. 6 Abs. 1 Buchstabe a DS-GVO ist die Einwilligung und wird deshalb gleich weggelassen.)

Die **Vertragserfüllung** sollte immer dann als Rechtsgrundlage gewählt werden, wenn schriftliche oder mündliche Verträge mit dem Betroffenen erfüllt werden, aber auch wenn vorvertragliche Maßnahmen erforderlich sind. Hierbei gilt es zwei Einschränkungen zu beachten, zum einen, dass es „auf Anfrage der betroffenen Person" erfolgen muss (dies ist der entscheidende Unterschied zur Werbung), zum anderen, dass der Betroffene selbst der Vertragspartner sein muss.

Beispiele für die Vertragserfüllung sind die Verwaltung der Mitgliederdaten im Verein, Lohnüberweisung, der Bewerbungsprozess im Unternehmen, Verkaufsabwicklungen (inkl. Versand) usw. Erweitert kann sogar davon ausgegangen werden, wenn ein Betroffener die Kommunikation initiiert und beispielsweise Unterlagen anfordert oder sich zu Schulungen anmelden möchte, dass es sich um Vertragserfüllung im Sinne der Datenschutz-Grundverordnung handelt.

Rechtliche Verpflichtung kommen immer dann zum Tragen, wenn in einem Gesetz steht, dass die Datenverarbeitung notwendig ist. Hierunter fallen beispielsweise Sozialversicherungsabgaben, Ausfuhrkontrollen, Aufbewahrungspflichten (d. h. elektronische und Papierarchive), Aktenvernichtung usw.

Die Option des **lebenswichtigen Interesses** als Rechtsgrundlage ist für die meisten Unternehmen und Vereine eher ohne Bedeutung. Hier sei nur angemerkt, dass wann immer mit Datenverarbeitung Leben gerettet werden kann, es also um Leben und Tod geht, der Datenschutz außen vor ist.

Die Rechtsgrundlage **öffentliches Interesse** betrifft vor allem Behörden und Institutionen, die im öffentlichen Bereich tätig sind. Beispielsweise ist es in europaweiten Forschungsprojekten gewünscht, dass die Öffentlichkeit über die Fortschritte und Ergebnisse des Projektes informiert wird.

Sollten Sie für Ihre Datenverarbeitung keine Rechtsgrundlage gefunden haben, dann kann Ihnen ggf. das **„berechtigte Interesse"** weiterhelfen. Besonders ist hierbei, dass es sich um die „berechtigten Interessen des Verantwortlichen oder eines Dritten" handeln kann.

Das berechtigte Interesse ist im ersten Schritt nach der Einwilligung eine schnelle Wahl des Verantwortlichen. Jedoch gilt es zu beachten, dass eine Abwägung im Vorfeld durchgeführt werden muss und hierbei die berechtigten Interessen des Verantwortlichen den schutzwürdigen Interessen des Betroffenen gegenübergestellt werden müssen. Auf diese Abwägung wird hier nicht näher eingegangen.

Dennoch wird sich viel auf genau diese Rechtmäßigkeit stützen können. Bei den berechtigten Interessen gibt es ähnlich wie bei der Einwilligung ein Widerspruchsrecht, welches aber eingeschränkt ist (vgl. Art. 21 DS-GVO). In der DS-GVO kann beispielsweise die Direktwerbung auch als ein mögliches berechtigtes Interesse begründet werden. In Deutschland sind jedoch noch andere Gesetzte zu beachten (z.B. TMG, UWG), an denen die Werbung aufgrund eines berechtigten Interesses scheitern kann.

Beispiele für berechtigte Interessen sind im Unternehmen die Bereitstellung von Arbeitsmitteln (Telefon, Internet, E-Mail) sowie die Erkennung und Abwehr von Angriffen (vgl. EWG 49 DS-GVO).

Bei der Ermittlung der Rechtsgrundlage können auch mehrere der oben genannten Möglichkeiten zutreffen. Die Entscheidung für eine Rechtsgrundlage sollte immer in den entsprechenden Verfahren dokumentiert werden.

Diese Abhandlung soll Sie ermutigen sich mit dem Thema Rechtsgrundlagen für Ihre Datenverarbeitungen im Unternehmen oder Verein näher zu beschäftigen und nicht automatisch bei der Einwilligung stehen zu bleiben. Beachten Sie zusätzlich auch die Grundsätze für die Verarbeitung von personenbezogenen Daten gemäß Art. 5 DS-GVO, da diese „parallel" zur Rechtmäßigkeit gelten. Die dort genannte Transparenz wird dann durch die Informationspflichten nach Art. 13 und Art. 14 DS-GVO erfüllt.

Über den Autor

Michael Schlagintweit
ist Begründer und Geschäftsführer der effiZERT GmbH. Zu seinen fachlichen Kernkompetenzen zählen der Datenschutz in KMU, Mitarbeitersensibilisierung und die Implementierung von ISMS und BCM.

▶ www.effizert.de

effiZERT
effizient zur Zertifizierung

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

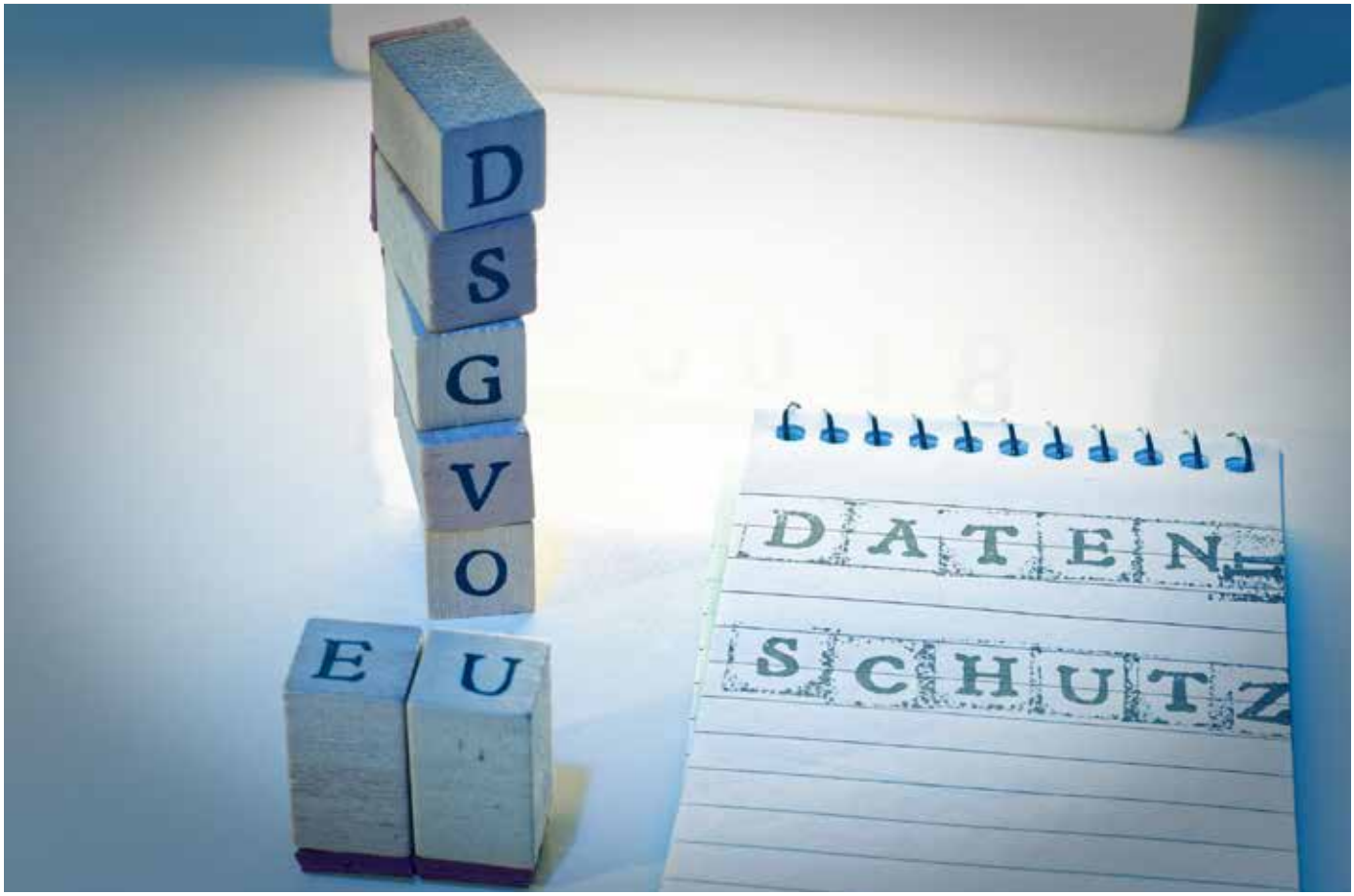
JETZT AUCH IN ENGLISCH

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

DAS KOPPLUNGSVERBOT UND DIE DS-GVO

Thomas Kahl, Rechtsanwalt, Taylor Wessing



Wenige Fragestellungen wurden vor dem Inkrafttreten der DS-GVO so kontrovers diskutiert wie die nach einem etwaigen Kopplungsverbot für (datenschutzrechtliche) Einwilligungserklärungen. Die Frage ist von erheblicher Tragweite. Nicht wenige Experten sehen hierin das Ende jedweder „datenfinanzierten" (Dienst-) Leistungen - vom kostenlosen Dienst im Web 2.0 bis hin zum kostenlosen Gewinnspiel. Trotz der grundlegenden Bedeutung und praktischen Tragweite der Fragestellung ist auch fast sechs Monate nach Inkrafttreten der DS-GVO keine Klärung in Sicht. Anlass, sich die wesentlichen Fragen und Lösungsansätze rund um das Kopplungsverbot nochmals zu vergegenwärtigen und zu fragen: Ist es wirklich so schlimm?

Kopplungsverbot – da war doch was!

Das Kopplungsverbot ist ein Begriff des Vertragsrechts. Er besagt, dass unter bestimmten Voraussetzungen das Abhängigmachen einer Leistung von einer anderen zum Schutze einer der Vertragsparteien oder der Allgemeinheit gesetzlich untersagt ist.

Das alte BDSG sah (wohl) kein generelles Verbot der Kopplung einer Vertragsleistung an die Abgabe einer datenschutzrechtlichen Einwilligungserklärung vor. Vielmehr existierte im alten Recht nur ein Sektor- bzw. Use Case spezifisches und deutlich beschränktes Kopplungsverbot, etwa in § 28 Abs. 3b BDSG (alt). Danach dürfte der Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen abhängig gemacht werden, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich war. Die Regelung wurde überwiegend als Kopplungsverbot in Monopolsachverhalten verstanden.

DS-GVO - Absolutes oder relatives Kopplungsverbot?

Im Zuge der Diskussion um ein mögliches Kopplungsverbot werden Art. 7 IV DS-GVO und EG 43 S. 2 der DSGVO ins Feld geführt, die auf den ersten Blick einem anderen Ansatz folgen: So soll dem Umstand der Koppelung der datenschutzrechtlichen Einwilligung an eine Leistung im Rahmen der Beurteilung der Freiwilligkeit der Einwilligung ***„in größtmöglichem Umfang Rechnung getragen werden"*** (vgl. Art. 7 (4) DS-GVO). Mit anderen Worten: Die Kopplung wird zum Beurteilungsmaßstab der Freiwilligkeit und somit auch der Wirksamkeit der Einwilligung.

Die Regelung des Art. 7 (4) DS-GVO reicht auf den ersten Blick weiter als die Vorgängerregelung im BDSG, stellt jedoch mit der darin enthaltenen Abwägungsregelung ***(„in größtmöglichem Umfang")*** ebenso klar, dass nicht jede Koppelung die Freiwilligkeit automatisch entfallen lässt. Erforderlich ist vielmehr eine Einzelfallprüfung, ob durch die Kopplung eine Situation entsteht, die die Freiheit zur Willensentschließung aufhebt. Ein absolutes Koppelungsverbot, dass bei jeder Art der Koppelung einer datenschutzrechtlichen Einwilligung mit anderen Leistungen zwangsläufig zur Unfreiwilligkeit der Einwilligung führt, dürfte danach ausscheiden.

Unklar ist in diesem Zusammenhang, welche Wirkung die ungleich striktere Formulierung in EG 43 S. 2 DS-GVO haben soll ***(„Die Einwilligung gilt nicht als freiwillig erteilt, wenn [...] die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.")*** oder ob nicht hierdurch ein absolutes Kopplungsverbot „durch die Hintertür" eingeführt wird. Nicht zuletzt die Leitlinien der EU-Gremien zur Abfassung von Rechtstexten der Europäischen Union sowie die Entstehungsgeschichte der jeweiligen Regelungen dürften den Schluss zulassen, dass die - deutlich entschärften - Kriterien in Art. 7 (4) DS-GVO maßgeblich sein sollen, so dass die Annahme eines bloß relativen Kopplungsverbots sachgerecht erscheint - die wesentliche Nachricht für alle betroffenen Unternehmen.

Folgt man diesem Ansatz, bleibt im Einzelfall zu bewerten, ab wann die Kopplung zur Unwirksamkeit der Einwilligung führt. Dabei dürften Monopol- und Monopol-ähnliche Fallgestaltungen auch weiterhin eine gewisse Indizwirkung für eine unzulässige Kopplung haben. Mangels ausdrücklicher Anhaltspunkte im Gesetz erscheint dies aber keinesfalls zwingend. Außerhalb dieses Bereichs dürften verschiedene Kriterien eine Rolle spielen. Die Unentgeltlichkeit der Leistung dürfte einen erweiterten Argumentationsspielraum pro Kopplung eröffnen, wobei die Grenzen umstritten sind. Fraglich bleibt zudem die Bewertung in Fällen bloß teilsubventionierter Leistungen, wobei auch hier eine Kopplung nicht ausgeschlossen sein dürfte.

Was sagen die Gerichte, was die Behörden?

Gerichtliche Entscheidungen hierzu sind weiterhin Mangelware. Der Oberste Gerichtshof in Österreich (OGH) äußerte sich in einem Urteil vom 31.08.2018 (Az. 6Ob140/18h) u.a. zur Wirkung des EG 43. Das Gericht scheint zwar ebenso ein bloß relatives Kopplungsverbots anzunehmen, gibt jedoch der strikteren Auslegung des EG 43 scheinbar den Vorzug und scheint den Spielraum der Norm damit einzuschränken, wobei Details unklar bleiben.

Belastbare Stellungnahmen der Datenschutzkonferenz - insbesondere im Hinblick auf die Frage des Umgangs mit der Kopplung bei kostenlosen Leistungen - fehlen bislang. . Dabei scheinen einige Landesbehörden das Konzept eines ▸

bloß relativen Kopplungsverbots kritisch zu sehen. Eine klare Linie lässt sich aber (noch) nicht erkennen. Gleichfalls unergiebig sind die bisherigen Stellungnahmen der europäischen Gremien wie der (früheren) Art. 29 Gruppe.

Das BayLDA skizzierte zuletzt in seiner Orientierungshilfe den in der Literatur vielfach vertretenen Ansatz, in Fällen kostenloser aber datenfinanzierter Leistungen den Weg über die sog. „Vertragslösung" zuzulassen. Hier wird die Hingabe personenbezogener Daten zum Gegenstand der Leistungspflichten des Betroffenen gemacht. Einer Einwilligung bedürfte es dann nicht mehr.

Kopplung - was geht noch, was nicht (mehr)?

Die Vielfältigkeit der offenen Fragen verdeutlicht das Dilemma, in dem sich betroffene Unternehmen befinden.

Ganz sicher gehen wird man letztlich nur durch strikte „Entkopplung" von Leistung und Forderung nach personenbezogenen Daten des Betroffenen. Dabei zeigt die Beratungspraxis, dass das Entkoppeln in manchen Fällen durchaus möglich und gangbar ist, aber oftmals das (ungeliebte) Überbordwerfen alter Konzepte erfordert.

Insbesondere im Bereich des Direktmarketings eröffnet § 7 Abs. 3 UWG gewisse Erleichterungen für die Email-Werbung, die im Einzelfall eine Einwilligung entbehrlich machen können. Hier zeigt die Beratungspraxis, dass viele Unternehmen die Grenzen des Möglichen oftmals schlicht aus Unkenntnis nur unzureichend ausloten.

Wo „einfache" Lösungen nicht in Betracht kommen, bleibt die weiterhin schwierige Abgrenzung zwischen erlaubter und nicht (mehr) erlaubter Kopplung im Einzelfall. Die gute Nachricht ist jedoch, dass hier entgegen erster Befürchtungen nicht alles verboten sondern einiges möglich bleiben wird. Die „Vertragslösung" des BayLDA scheint ein pragmatischer, wenngleich nicht ganz unkomplizierter Ansatz, da insbesondere im Bereich der Transparenz hohe Hürden bestehen bleiben und die Frage der „Bezahlung" mit Daten im Einzelfall zu nicht ganz einfachen rechtlichen Abgrenzungs- und Folgefragen führen dürfte. Schon aus diesem Grund dürfte in Fällen kostenloser Leistungen weiterhin die „echte" gekoppelte Einwilligung auch weiterhin eine gewisse praktische Bedeutung behalten, wo die Einzelfallabwägung „positiv" ausfällt.

Fazit

Es bleibt abzuwarten, wie sich die Aufsichtsbehörden zu den offenen Fragestellungen positionieren. Betroffene Unternehmen sollten die Entwicklungen aufmerksam beobachten. Bis dahin bleibt es betroffenen Unternehmen unbenommen, von den bestehenden Auslegungsspielräumen Gebrauch machen. Sinnvolle Lösungen bleiben möglich. Und das klingt doch erstmal gar nicht so schlecht!

Über den Autor

Thomas Kahl
Rechtsanwalt, Taylor Wessing
Der Autor ist Rechtsanwalt und Salary Partner der internationalen Wirtschaftskanzlei Taylor Wessing am Standort Frankfurt. Er berät nationale wie internationale Unternehmen zu Fragen des Datenschutzes, der IT-Sicherheit und Compliance im Rahmen der Ausgestaltung von (konzernweiten) Datenverarbeitungsprozessen und aufsichtsbehördlichen Verfahren.

▶ www.taylorwessing.com

TaylorWessing

Anzeige

DSGVO KONFORM*

*Schreddern unterstützt die Einhaltung der DSGVO.

Was tun Sie für die Sicherheit Ihrer Papierdokumente?

Schreddern unterstützt die Einhaltung der DSGVO.

Jetzt auf ausgewählte Geräte Cashback sichern bis 31.12.2018

Mehr auf: www.rexeleurope.com

Mit automatischen Aktenvernichtern sparen Sie 98 % Ihrer Zeit

Die neue europäische Datenschutzgrundverordnung (DSGVO) betrifft auch Papierdokumente und bedeutet, dass wir mehr Schreddern sollten. Dies muss aber nicht zu Lasten Ihrer kostbaren Arbeitszeit fallen. Im Vergleich zu herkömmlichen, manuellen Aktenvernichtern, sparen Sie mit den Rexel Auto+ Aktenvernichtern bis zu 98% der Zeit für das Schreddern*.

www.rexeleurope.com

*Unabhängige Studie von Intertek Testing & Certification Ltd

Rexel®
THE CLEVER CHOICE

LÖSCHUNG IM LICHTE DER NEUEN DATENSCHUTZ-GRUNDVORORDNUNG (DS-GVO)

Interview mit Gerhard Friederici

Mit Einführung der DS-GVO ist das Bewusstsein von Datenschutz in Unternehmen rapide angestiegen. Das Wissen über Datenlöschung ist aber oft noch sehr lückenhaft. Was hier zu beachten ist, erläutert Gerhard Friederici. Er ist seit 18 Jahren Datenschutzbeauftragter der Rhenus-Gruppe, einem der größten Anbieter im Bereich Dokumentenmanagement.

Herr Friederici, wie hat sich Ihr Arbeitsgebiet mit der Einführung der neuen Europäischen Datenschutz-Grundverordnung DS-GVO im Mai dieses Jahres verändert?

Zunächst einmal: Ja, die Arbeitsintensität ist seit dem 25. Mai, seitdem die DS-GVO für alle gültig ist, sehr deutlich gestiegen. Auch das Arbeitsfeld hat sich enorm erweitert. Denn neben der internen Bewältigung der rechtlichen Vorgaben – bei Rhenus mussten mehrere Tausend Verträge angepasst werden – hat vor allem die Zahl der datenschutzrechtlichen Fragen von Kunden deutlich zugenommen. Denn es geht nicht allein darum, was im Gesetz steht, sondern vor allem darum, wie die Anforderungen angemessen im Geschäftsleben umgesetzt werden können. Die richtige Frage lautet daher oft: Welche Maßnahmen muss ich ergreifen, um ein Risiko handhabbar zu machen?

Was bedeutet das konkret für die Löschung von Daten? Welche Rechtsgrundlagen gibt es dafür?

In den meisten Unternehmen ist die Mentalität des Datensammelns stark ausgeprägt. Gerade im Kontext von Industrie 4.0 und Digitalisierung sind nicht nur Staat und Behörden, sondern vor allem Unternehmen bemüht aus einer Fülle von Daten die richtigen Informationen zu generieren. Andererseits sind aber auch viele Verbraucher bereit ihre persönlichen Daten leicht weiterzugeben. Wir sind heute Weltmeister im Daumenbewegen am Smartphone. Daher kommt es darauf an hier das Bewusstsein für den Datenschutz zu schärfen und zugleich die Betroffenenrechte stärken. Ihnen ist in der DS-GVO ein separater Bereich gewidmet, der Artikel 17, in dem es um das „Recht auf Vergessenwerden" geht. Ich will hier klar sagen: Für Unternehmen ist das Löschen an sich kein neues Thema. Es hat nur eine wesentlich höhere Wahrnehmung mit der DS-GVO bekommen, weil hier erstmals die Bußgelder hoch sind.

Warum ist gerade die Löschung von Daten so enorm wichtig zur Umsetzung der DS-GVO?

Die DS-GVO hat für alle Bürger die Informations- und Auskunftsrechte gestärkt. Der damit verbundene Anspruch auf Richtigstellung oder Löschung von Daten kollidiert aber mit der Datensammelwut von Unternehmen. Denn es gilt der Grundsatz: Jede Verarbeitung meiner Daten ist grundsätzlich verboten, es sei denn, die Verarbeitung ist rechtmäßig. Das kann, zum Beispiel, eine konkrete Erlaubnis sein. Schon das alte Bundesdatenschutzgesetz kannte dieses Verbot mit Erlaubnisvorbehalt. Er wurde jetzt noch einmal deutlich verschärft. Um die Verarbeitung von Daten zu rechtfertigen, ziehen Unternehmen gern das sogenannte berechtigte Interesse heran. Aber das ist zu kurz gegriffen. Es muss einen Interessensausgleich geben. Das ist Aufgabe des Verantwortlichen. Um es also ganz klar zu formulieren: Wenn es keinen Interessenausgleich gibt, dann ist die Rechtmäßigkeit der Datenerhebung nicht gegeben, dann muss gelöscht werden. Das gleiche gilt natürlich auch, wenn der Betroffene seine Einwilligung zurückzieht, dann muss ebenfalls gelöscht werden. Kurzum: Die Rechte des Betroffenen müssen umgesetzt werden können.

Können Sie uns angesichts der neuen gesetzlichen Vorgaben sagen, wie ein Löschvorgang im Unternehmen am besten organisiert werden sollte?

Ein Stück Papier hilft auf Dauer nicht weiter. Wichtig ist, ein umfassendes Datenschutzmanagement aufzubauen. Zunächst sind dafür die klassische W-Fragen zu stellen:

Welche Daten gibt es in welchem System und warum, wo liegen sie überall, wer hat Zugriff darauf und welche Aufbewahrungsfristen gelten für welche Datensätze? Erst wenn ich diese Antworten habe, kann ich geeignete Löschmethoden wählen. Innerhalb der IT bietet sich an, Löschprogramme aufzusetzen, die das personenbezogene Datum aus Segmenten oder ganzen Datenbanken löscht. Eine weitere Methode kann sein, dass die Datenträger physisch vernichtet werden. Aber hier geht das Problem schon los. Wie finde ich diese Daten überhaupt? Denn wir reden ja nicht nur über aktuelle Daten, sondern auch über elektronische Alt-Archive, über Back-up-Systeme und nicht zuletzt über Daten, die ganz altmodisch in Ordnern in Kellerregalen oder Panzerschränken stehen. Ein Löschkonzept heißt also, verbindliche Regeln aufzustellen, wie mit verschiedenen Datenträgern, Löschungsfristen und Gesetzesvorgaben in Summe umgegangen werden soll. Denn wenn der Zweck der Verarbeitung entfallen ist, muss gelöscht werden.

Datenlöschung ist offenbar eine Sisyphusarbeit. Was kann man tun, um angesichts der Komplexität nicht zu verzweifeln?

Zur Umsetzung der Betroffenenrechte sollten die Daten in größeren Kategorien verdichtet und klassifiziert werden. Wer hier Artikel 30 schon angewendet hat, wonach jede Datenverarbeitung dokumentiert werden muss – auch mit Einstufung der Sensibilität der Daten –, der ist schon einen großen Schritt weiter. Denn aus der Risikobetrachtung werden Schutzbedarf und Schutzmaßnahmen abgeleitet. All diese Ergebnisse werden schließlich in eine Risiko-Matrix übertragen, die dann beschreibt, welche technischen oder organisatorischen Maßnahmen anzuwenden sind, damit diese Daten bei Bedarf gelöscht werden können. Löschklassen werden also aus dem Schutzbedarf heraus aufgestellt. Eine gute Hilfestellung zur Umsetzung eines Löschkonzeptes gibt mittlerweile die DIN 66398. Zur Verfahrensbeschreibung gehört natürlich auch eine Risikofolgenabschätzung. Der letzte Schritt ist dann die organisatorische Anweisung an die Fachabteilung diese Löschregeln umzusetzen und gegebenenfalls die Datenträger zu vernichten.

Immer wieder tauchen Meldungen über „Daten in der Mülltonne“ auf. Was heißt datenschutzgerechte Vernichtung von Datenträgern nach dem Stand der Technik?

Kein Mensch möchte, dass sich seine Steuerdaten oder medizinischen Unterlagen im Müll wiederfinden. Deshalb gibt es für die Vernichtung anerkannte Regeln, den sogenannten Stand der Technik. Hier empfiehlt sich ein Blick in die DIN 66399, wo nicht nur Schutzklassen definiert sind, sondern auch beschrieben ist, wie der Prozess von Abholung und Vernichtung technisch-organisatorisch umzusetzen ist. Alles ist standardisiert und normiert. Die Schutzklassen spiegeln dabei die Angemessenheit wieder, was sich wiederum aus der Risikobewertung ergibt. Auch international hat sich mittlerweile mit der ISO 21964 eine Standardnorm entwickelt, wie der Prozess der Datenträgervernichtung nach Stand der Technik umgesetzt werden sollte. Dabei geht es um eine Zuordnung zu Schutzklassen und Sicherheitsstufen. Die sieben Sicherheitsstufen beschreiben hier die Größe der letztendlichen Partikel – verbunden mit unterschiedlichen Materialcodes. Sollte die Datenvernichtung durch einen Dienstleister erfolgen, reicht es aus, dass in dem Vertrag gefordert wird, normenkonform nach Stand der Technik zu arbeiten. Im operativen Umsetzungskonzept müssen also nur noch die Schutzklassen definiert werden, der Rest ergibt sich von allein. ▸

Welche praktischen Erfahrungen haben Sie in den vergangenen Monaten gemacht? Haben Sie Tipps für Datenschutzbeauftragte, was beim Thema Daten-Löschung zu beachten ist?

Ein guter Datenschutzbeauftragter ist einer, der nicht nur sagt, was im Gesetz steht, sondern durch ständig aktualisiertes Wissen und im Austausch mit anderen Datenschutzexperten sowie in Zusammenarbeit mit der eigenen Geschäftsführung herausfindet, wie die Vorgaben datenschutzkonform umgesetzt werden können. Denn ein Datenschutzbeauftragter ist eine zusätzliche Kontrollinstanz. Und er ist auch persönlich haftbar, wenn er wegsieht. Denn die Ausrede, es sei noch nie etwas passiert, ist Selbstbetrug. Dann kommt nicht die Frage, wie konnte es passieren, sondern was haben Sie getan, damit es nicht passiert. Und auf unser Thema bezogen heißt das: Datenlöschung ist kein Einzelvorgang, sondern ein Konzept. Hier gilt der Dreiklang: organisieren, kontrollieren, dokumentieren. Das ist manchmal unbequem. Aber ein Datenschutzbeauftragter darf nicht bei jedem kleinen Windstoß umfallen.

Zum Abschluss: Was sagen Sie gerade klein- und mittelständischen Unternehmen, warum sie auf die Einhaltung der DS-GVO-Vorgaben zur Löschung achten sollten?

Man kann Vorgaben ignorieren – genauso, wie Sie jederzeit gern blind über die Autobahn laufen können. Sie müssen dann nur mit den Konsequenzen leben. Deshalb ist jeder Unternehmensleiter gut beraten, eine Risikoabwägung vorzunehmen – immer im Kontext der Daten, die er verarbeitet und welche Schutzmaßnahmen dafür erforderlich sind. Ja, Sicherheit kostet Geld.

Aber wer nicht nach dem Angemessenheitsprinzip handelt, begeht einen Vorsatz und das kann als Straftat oder Ordnungswidrigkeit und mit einer Haftung bis zu einer Million Euro geahndet werden. Aber es geht nicht einmal primär um die Kosten, sondern um die Frage, wie stelle ich mich als Unternehmen der sozialen Verantwortung. Der Datenschutz wird somit ein Teil dieser Compliance-Umsetzung und damit letztlich auch zu einem Wettbewerbsvorteil.

Über den Interviewpartner:

Gerhard Friederici
Leitung Sicherheit und Qualität
Rhenus Office Systems GmbH

▶ www.office-systems.de

JOINT CONTROLLERSHIP-VEREINBARUNGEN (JC-V) – NICHT AUSNAHME, SONDERN REGEL

Rechtsanwalt Karsten U. Bartels LL.M.

Die EuGH-Entscheidung zu den datenschutzrechtlichen Folgen der Nutzung von Facebook Fanpages (Urteil vom 05.06.2018, C-210/16) hat signifikante Auswirkungen auf die Gestaltung von und Beratung zu **kooperativer Datenverarbeitung**. Aus deutscher Sicht gab es wohl die heimliche Hoffnung, Art. 26 DS-GVO spiele keine, jedenfalls eine unwesentliche Rolle. Das ist historisch nachvollziehbar, da das alte BDSG keine nationalstaatliche Regelung zur **gemeinsamen Verantwortlichkeit** kannte, obwohl dieses Modell in der EU-Datenschutzrichtlinie angelegt war. Die Entscheidung des EuGH ist sehr bedenklich, zeigt aber, wie tendenziös unsere Sicht bislang war. Insbesondere die kooperative Verarbeitung von personenbezogenen Daten im Zwei-Parteien-Verhältnis wird bislang nahezu immer als Auftragsverarbeitung im Sinne von Art. 28 DS-GVO qualifiziert. Es gilt zu realisieren: Die DS-GVO stellt **zwei Modelle** zur Verfügung, um Dritte ordnungsgemäß in die gewünschte Datenverarbeitung einzubeziehen. Diese beiden Konstruktionen stehen weder in einem Regel-Ausnahme-Verhältnis zueinander, noch gibt es einen Anwendungsvorrang von Art. 28 DS-GVO.

Der Umgang mit Art. 28 DS-GVO bereitet noch einige Schwierigkeiten, der mit Art. 26 DS-GVO einige mehr. Die folgenden Ausführungen widmen sich deshalb den Anforderungen des Art. 26 DS-GVO:

Voraussetzung einer gemeinsamen Verantwortlichkeit (Joint Controllership bzw. Joint Controllers) ist nach Art. 26 Abs. 1 S. 1 DS-GVO die **gemeinsame Festlegung der Mittel und Zwecke** der Datenverarbeitung durch **zwei oder mehr Verantwortliche**. Ist ein an der Datenverarbeitung Beteiligter nicht Verantwortlicher im Sinne von Art. 4 Ziff. 7 DS-GVO, kann er noch Auftragsverarbeiter sein, nicht aber einer von mehreren Joint Controllers. Art. 26 DS-GVO stellt – eben so wenig wie Art. 28 DS-GVO für die Auftragsverarbeitung ▸

– keine Rechtsgrundlage für die Verarbeitung durch mehrere Verantwortliche dar. Folglich benötigt **jeder Verantwortliche eine eigene Rechtsgrundlage** für die Verarbeitung (Art. 6 DS-GVO). Einer Rechtsgrundlage für die Nutzung der Joint-Controllership-Konstruktion selbst bedarf es nicht.

Die Verantwortlichen haben festzulegen, welcher Verantwortliche welche Pflicht nach der DS-GVO erfüllt. Diese Joint-Controllership-Vereinbarung („JC-V" oder „JCA", stehend für Joint Controllership Agreement) zeitigt **keine konstitutive Wirkung**. Vielmehr ist die Pflicht zur Vereinbarung schlicht bußgeldebewehrte Rechtsfolge, Art. 83 Abs. 4 lit. a DS-GVO.

Die Möglichkeit, mehrere und unter den Verantwortlichen auch gerade **unterschiedliche Zwecke** festlegen zu können, erlaubt es auch, komplexe und multilaterale Datenverarbeitungsprozesse datenschutzkonform aufzusetzen. Unterschiedliche Zwecke ermöglichen – abweichend von der Auftragsverarbeitung, bei der grundsätzlich „fremde" Daten zu fremden Zwecken verarbeitet werden – die Verarbeitung „fremder" Daten zu eigenen Zwecken und „eigener" Daten zu fremden Zwecken. Die Festlegung der **Mittel** lässt es unter anderem zu, gemeinsame Ressourcen einzusetzen, also die Datenverarbeitung technisch auf die IT-Systeme der Verantwortlichen zu verteilen.

JC-Vereinbarungen müssen hinsichtlich der Festlegung der Zwecke und Mittel der Verarbeitung weder gleichberechtigt zustande gekommen sein noch diese materiell gleichberechtigt regeln.[1] Eine solche Symmetrie ist im Gesetz nicht angelegt und machte eine Anwendung der Norm nahezu unmöglich. Die Parteien sind in ihrer Vertrags- und Verfahrensgestaltung frei.

Demgemäß ist es auch rechtlich zulässig, **Unterauftragnehmer** in die Verarbeitung einzubeziehen, soweit dies in der JC-Vereinbarung bestimmt ist. Es ist also zulässig, als Verantwortlicher in einer JC-Konstellation **zugleich Auftraggeber einer Auftragsverarbeitung** nach Art. 28 DS-GVO zu sein, im Rahmen derer der Auftragsverarbeiter eine Verarbeitung übernimmt, die Teil der JC-Verarbeitung ist. Diese Erkenntnis scheint trivial, ist aber wesentlich.

Eine gemeinsame Verantwortlichkeit kommt beispielsweise in Frage bei gemeinsamen Aufbau und Nutzen einer **Datenbank**; gemeinsame Nutzung von Adressdaten; **Internet-Portale**, die von mehreren Unternehmen oder Behörden gemeinsam betrieben werden; Software-Anwendungen oder andere **IT-Ressourcen**, die von konzernverbundenen Unternehmen gemeinsam betrieben und genutzt werden. Auch die gemeinsame Erstellung und Verwertung von **Studien** oder **Industrie 4.0-Anwendungen**, wie z. B. komplexe Fertigungs- oder Logistikprozesse kommen in Betracht. Und, wie der EuGH zeigt, sogar die bilateral vereinbarte Nutzung von **Social Media**.

Art. 26 DS-GVO regelt den notwendigen Inhalt einer JC-Vereinbarung. Danach sind die Verantwortlichen zu bestimmen, die Mittel und Zwecke der Verarbeitung festzulegen und die datenschutzrechtlichen Pflichten aufzuteilen, insbesondere hinsichtlich der Erfüllung der Informationspflichten nach Artt. 13 f. DS-GVO und der Betroffenenansprüche auf Auskunft, Berichtigung, Löschung, Datenportabilität und Widerspruch. Die Kürze der gesetzlichen Regelung trügt. JC-Verträge haben die Datenverarbeitung umfänglich (**„tatsächliche Funktionen und Beziehungen"**, Art. 26 Abs. 2 S. 1 DS-GVO) zu beschreiben, also die technische Arbeitsteilung und die Verfahren derart darzulegen (**„in transparenter Form"**, Art. 26 Abs. 1 S. 2 DS-GVO), dass sie dadurch prüfbar sind und die Betroffenen ordnungsgemäß informiert werden.

Ein besonderes Augenmerk verdienen dabei die Regelungen über die **technischen und organisatorischen Maßnahmen**. Sie sind nach den Anforderungen der Artt. 5 Abs. 1 lit. f; 24 Abs. 1 und 32 DS-GVO einzurichten und zu unterhalten und als „Mittel der Verarbeitung" in der JC-Vereinbarung festzulegen. Die nach Art. 32 DS-GVO komplexen Fragestellungen zur ordnungsgemäßen Berücksichtigung des **Stands der Technik**[2], der **Wirksamkeitsprüfung**, der datenschutzrechtlichen(!) **Schutzbedarfsanalyse**, der **Dokumentation** und der **Kontrolle** führen in einer komplexen Datenverarbeitung zu umfänglichen, anspruchsvollen Regelungen. Zwecks Übersichtlichkeit sollten derartige Regelungen mit Visualisierungen o. ä.

[1] A. A. wohl Lachenmann in Lachenmann/ Koreng, Formularhandbuch Datenschutzrecht, 2. A. 2018, Art. 26 Anm. 1.

[2] Karsten U. Bartels, Unterschreiten des Stands der Technik - Entscheidungsspielräume und Rechtsfolgen von Fehlentscheidungen nach Datenschutz-Grundverordnung und IT-Sicherheitsgesetz, BvD-News Ausgabe 03/2017, S. 50; Karsten U. Bartels/ Michael Schramm, Neue Anforderungen zum technischen Datenschutz nach der Datenschutz-Grundverordnung, BvD-News 1/2017, S. 22.

flankiert werden. Die denkbaren Fallgestaltungen gehen inhaltlich deutlich weiter auseinander als das bei AV-Vereinbarungen vorstellbar ist. So nimmt es nicht wunder, dass es zumindest bislang keine Muster-JC-Vereinbarungen gibt, die den Anspruch haben dürfen, einigermaßen universell zum Einsatz zu kommen. Nicht übersehen: Soweit ein Verantwortlicher zur Erfüllung der ihn treffenden **Meldepflichten** nach Art. 33 DS-GVO auf Zuarbeit eines anderen Verantwortlichen angewiesen ist, sollte das dafür erforderliche Verfahren sogleich mit geregelt werden.

Optional kann die Einrichtung einer **gemeinsamen Anlaufstelle** für die Betroffenen vereinbart werden, Art. 26 Abs. 1 S. 3 DS-GVO. Die gemeinsame Anlaufstelle soll es der betroffenen Person erleichtern, ihre Rechte geltend zu machen, indem sie sich an einen ausgewiesenen Ansprechpartner, der kein Dritter ist, wenden kann.

Art. 26 Abs. 2 S. 2 DS-GVO verpflichtet die Verantwortlichen, den Betroffenen **das Wesentliche der Vereinbarung zur Verfügung zu stellen**. Es handelt sich damit um eine limitierte Informationspflicht, nicht um eine allgemeine „Veröffentlichungspflicht". Den Maßstab der Wesentlichkeit benennt die Norm nicht. Da die besondere Informationspflicht aber ausschließlich dem Betroffenen nutzen soll, kommt es bei der **Feststellung der Wesentlichkeit** auch lediglich auf seine Perspektive an. Die Wesentlichkeit kann sich allerdings nicht in der Verteilung der Erfüllungspflichten der Betroffenenansprüche erschöpfen. Denn die Erfüllung dieser Ansprüche kann der Betroffene ohnehin von jedem einzelnen Verantwortlichen fordern, Art. 26 Abs. 3 DS-GVO. Solange wir zum gesetzlich erforderlichen Umfang keine gerichtliche Klärung verzeichnen können, sollte die Information zumindest auch den oben beschriebenen Inhalt zu den „tatsächlichen Funktionen und Beziehungen" enthalten. Ebenso sind die Regelungen über die vereinbarten **Zwecke** offenzulegen, damit die Zuordnung zu den Verantwortlichen ein-eindeutig nachvollzogen werden kann. Die vereinbarten Mittel hingegen auszunehmen ist vertretbar, da ein Vergleich mit der Auftragsverarbeitung zeigt, dass der Betroffene im Rahmen einer ihn betreffenden Auftragsverarbeitung dort auch dann keinen Anspruch auf Offenlegung der eingesetzten **Mittel** hat, wenn die Datenverarbeitung durch weitere Unterauftragnehmerstufen rechtlich und technisch sehr komplex ausgestaltet ist. Es ist nicht erkennbar, warum der Betroffene insoweit anders gestellt sein soll.

Die gemeinsame Verantwortlichkeit verpflichtet nicht grundsätzlich zur Durchführung einer **Datenschutz-Folgenabschätzung** nach Art. 35 DS-GVO. Eine Verarbeitung nach Art. 26 DS-GVO wurde auch nicht in die „DSFA Liste Deutschland" für den nicht-öffentlichen Bereich aufgenommen.

Fazit in Arbeitsthesen:

1. Eine kooperative Datenverarbeitung bedingt die aktive Auswahl des zutreffenden Modells nach Art. 26 bzw. Art. 28 DS-GVO.
2. Das Joint-Controllership-Modell ist keine zu rechtfertigende Ausnahme. Es steht neben der Auftragsverarbeitung.
3. Die Prüfung sollte dokumentiert werden.
4. Die Vertragsgestaltung ist in der Regel individuell und tendenziell komplex.
5. Joint Controllership eröffnet die Möglichkeit zur kreativen Gestaltung komplexer Datenverarbeitung.

Über den Autor

Karsten U. Bartels LL.M.
Rechtsanwalt, HK2 Rechtsanwälte
Vorstand Bundesverband
IT-Sicherheit e. V. (TeleTrusT)

- www.hk2.eu
- www.it-sicherheit-und-recht.de
- www.teletrust.de

TeleTrusT Pioneers in IT security. Bundesverband IT-Sicherheit e.V.

HK2 Rechtsanwälte

ÜBERWACHUNG – DIE UNBEKANNTE AUFGABE?

Dr. Niels Lepperhoff

I. Einleitung

Zu den in Art. 39 Abs. 1 lit. b) DS-GVO festgelegten Aufgaben des Datenschutzbeauftragten (DSB) gehört die „Überwachung der Einhaltung dieser Verordnung […]". Diese Überwachungsaufgabe des DSB ergänzt die Verantwortung des Verantwortlichen, die getroffenen Maßnahmen zur Einhaltung der DS-GVO zu überprüfen (Artt. 24 Abs. 1 S. 2 und 32 Abs. 1 lit. d) DS-GVO). Überwachung bezieht sich sowohl auf eine Prüfung der vom Verantwortlichen selbst durchgeführten Kontrollen, als auch auf eigene Prüfhandlungen des DSB.

Die Überwachungsaufgabe gehört zu den Pflichtaufgaben des DSB (vgl. auch BvD Berufsleitbild, Kapitel 3.4). Ein Versäumen der Überwachungstätigkeit ist mit einem Bußgeld zu Lasten des Verantwortlichen bewehrt (Art. 83 Ab. 4 lit. a) DS-GVO). Für uns DSB eröffnet sich damit eine zusätzliche Möglichkeit, uns unbeliebt zu machen. Flapsig formuliert nimmt der DSB nicht nur das Spielzeug weg, sondern petzt auch noch bei den Eltern.

Die Überwachung lässt sich in der Kommunikation mit Betroffenen – und Auftraggebern im Rahmen einer Auftragsverarbeitung – positiv verwenden. Die Überwachung dient als Nachweis, dass insbesondere die Anforderungen der DS-GVO erfüllt werden.

Gute Gründe also, sich die Frage zu stellen: wie lässt sich die Überwachungsaufgabe in der Praxis umsetzen?

II. Welche Rechtsgrundlage trägt die Überwachungstätigkeit?

Im Rahmen der Überwachung werden personenbezogene Daten verarbeitet. Beispielsweise bei einer Prüfung, ob Zugriffsrechte im Einklang mit Art. 25 Abs. 2 DS-GVO minimal vergeben wurden, ist ein personenscharfer Zugriff auf die vergebenen Zugriffsrechte erforderlich.

Aus Platzgründen und mit Blick auf die praktische Relevanz konzentriert sich der Beitrag auf „normale" personenbezogene Daten. Die Besonderheiten der Artt. 9 und 10 DS-GVO sowie § 24 BDSG sollen hier nicht behandelt werden.

Die auszuwertenden Daten wurden auch zur Überwachung erhoben

Eine Einwilligung (Art. 6 Abs. 1 lit a) DS-GVO) scheitert regelmäßig an dem Machtungleichgewicht im Unternehmen und würde die Überwachungstätigkeit in das Belieben des Überwachten stellen. Es liegt auf der Hand, dass für die Erfüllung eines Vertrags mit den Betroffenen eine Überwachung auf Einhaltung der DS-GVO grundsätzlich nicht erforderlich ist (Art. 6 Abs. 1 lit b) DS-GVO). Ein Gesetz, dass im Sinn des Artt. 6 Abs. 1 lit c) i.V.m. Abs. 3 DS-GVO die Verarbeitung von personenbezogenen Daten im Rahmen der Überwachungsaufgaben anordnet oder erlaubt, ist nicht erkennbar. Art. 6 Abs. 1 lit. d) und e) DS-GVO sind offensichtlich ebenfalls nicht einschlägig. Letztlich bleibt regelmäßig die Interessensabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO, um die Verarbeitung personenbezogener Daten im Rahmen der Überwachungstätigkeiten zu legitimieren.

Welche personenbezogenen Daten verarbeitet werden, hängt von der konkreten Überwachungshandlung ab. Insofern ist die Interessensabwägung jeweils im Einzelfall durchzuführen. Grundsätzlich kann sie sich entlang der folgenden Argumentationslinie bewegen.

Auf Seiten des Verantwortlichen liegt das berechtigte Interesse in der Waagschale, die Anforderungen des Art. 39 Abs.1 lit. b) DS-GVO einzuhalten. Das Interesse am Einhalten einer gesetzlichen Vorschrift ist zweifelsohne berechtigt. Der Betroffene legt sein Interesse, dass seine Daten nicht zu diesem Zweck verarbeitet werden, in die andere Waagschale. Ohne eine Auswertung lässt sich die Überwachungsaufgabe nicht durchführen. Die Überwachung dient mittelbar dem Schutz der Rechte und Freiheiten des Betroffenen. Insofern dürfte das berechtigte Interesse des Verantwortlichen überwiegen.

Die auszuwertenden Daten wurden nicht zur Überwachung erhoben

Ob die Verarbeitung zulässig ist, hängt vom Ausgang des Kompatibilitätstest nach Art. 6 Abs. 4 DS-GVO ab. Da die zu berücksichtigenden Faktoren sehr stark vom Einzelfall abhängen, lässt sich keine generelle Aussage zur Zulässigkeit treffen.

Mit Blick darauf, dass der Kompatibilitätstest der Zweckänderung Grenzen zieht, ist es überlegenswert, die Überwachungsaufgabe als zusätzlichen Erhebungszweck festzulegen und in den Informationspflichten nach Art. 13 und 14 DS-GVO aufzunehmen.

III. Praktische Umsetzung der Überwachung

Auf welche Art und Weise ein DSB seiner Überwachungsaufgabe nachkommt, liegt in seinem Ermessen. Da die Zielsetzung der Überwachung ist, die Einhaltung von Regeln zu prüfen, bietet sich an, Vorgehensweise aus anderen Professionen, die ebenfalls Compliance-Prüfungen durchführen, zu adaptieren. Ein naheliegendes Beispiel ist die Revision.

Ohne Anspruch auf Vollständigkeit werden im Folgenden ausgewählte Aktivitäten skizziert. Die Darstellung erfolgt verallgemeinert und nicht bezogen auf ein bestimmtes Vorgehensmodell.

Voraussetzung

Die Überwachung stellt sich als Prüfungsprozess dar. Im Zentrum steht zu prüfen, ob gesetzliche und interne Vorgaben zum Datenschutz eingehalten werden. Zu den internen Vorgaben zählen Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen, elektronische Workflows usw. Die zu prüfenden internen Vorgaben müssen vorher erstellt worden sein. Das bedeutet im Umkehrschluss, dass eine Überwachung erst dann einsetzen kann, wenn Vorgaben bestehen.

Vorbereitung: Erstellung des Überwachungsplans

Das Ergebnis der Vorbereitung ist ein Überwachungsplan, der darlegt,

- welche Vorgabe geprüft werden soll,
- in welchen Intervallen die Prüfung der Vorgabe stattfinden soll und
- wer die Prüfung durchführen soll.

Grundsatz der Aufgabenerfüllung durch den DSB ist die Risikoorientierung nach Art. 39 Abs. 2 DS-GVO, d. h. den mit den Verarbeitungsvorgängen verbundenen Risiken unter Berücksichtigung von Umfang, Umständen und Zwecken der Verarbeitung sind gebührend Rechnung zu tragen.

Je nach Organisation erscheint die Überwachungsaufgabe neu. Deshalb empfiehlt es sich, die oberste Leitung frühzeitig in die Erstellung des Überwachungsplans einzubeziehen. Dadurch soll die Akzeptanz und Unterstützung durch diese erreicht werden. Für die Geschäftsführung kann eine Überwachung helfen die Sicherheit zu erhalten, so dass die Datenschutzvorgaben eingehalten werden. Eine Unterstützung durch diese hilft die aus der Überwachung resultierenden Folgeaktivitäten, beispielsweise zur Mängelbeseitigung, umzusetzen.

Auswahl der Regeln

Es bietet sich an in einem ersten Schritt die zu überwachenden Regelungen zu ermitteln.

Auswahl der stellvertretenden Verfahren oder Softwaresysteme

Regelungen werden immer in einem konkreten Verfahren umgesetzt oder nicht. Insofern bietet es sich an für die zu überwachenden Regelungen festzulegen, welche Verfahren oder Verfahrensschritte stellvertretend geprüft werden sollen. Alternativ können statt der Verfahren auch Softwaresysteme verwendet werden, wenn damit das Prüfungsziel zweckmäßiger erreicht werden kann.

Risikobewertung

Die für die Überwachung ausgewählten Paare „Regeln-Verfahren“ bzw. „Regel-Softwaresystem“ sind nach ihren Risiken zu klassifizieren. Bei der Risikobeurteilung ist der DSB frei, weitere Faktoren zu berücksichtigen. Er kann beispielsweise auch berücksichtigen, wie gut die verantwortlichen Personen in der Vergangenheit Datenschutzvorgaben eingehalten haben.

Prüfintervalle festlegen

Im nächsten Schritt werden die Prüfintervalle, z.B. wöchentlich, monatlich oder jährlich, festgelegt. Wenn es sich um eine Überwachung der Kontrolltätigkeiten des Verantwortlichen handelt, lässt sich ein längeres Intervall rechtfertigen als bei einer unmittelbaren Prüfung. ▸

Prüfer bestimmen

Für jede geplante Überwachung wird mindestens ein Prüfer benötigt. Auch wenn die Überwachung zu den Aufgaben des DSB zählt, muss der DSB nicht zwingend die Überwachung persönlich durchführen. Er kann die Aufgabe, wie jede andere ihm zugewiesene Aufgabe, an sein Hilfspersonal delegieren oder zur Unterstützung externe Fachkräfte heranziehen.

Idealerweise versteht ein Prüfer die zu prüfende Regel und das ausgewählte Verfahren fachlich. Bei einer rechtlichen Regelung kann ein juristischer Hintergrund hilfreich sein, bei eher technischen Regelungen, z. B. aus dem Bereich Sicherheit, ist ein technischer Hintergrund sachgerechter. Ein fachliches Verständnis hilft, die Antworten und Dokumente der zu prüfenden Bereiche inhaltlich zu verstehen und auch zu hinterfragen. Ohne ein fachliches Verständnis besteht die Gefahr, die Überwachung auf einen rein formalen Akt zu reduzieren. Folgende pointierte Darstellung illustriert den Unterschied: Als Antwort auf die Prüfungsfrage „Gibt es ein Sicherheitskonzept nach Art. 32 Abs. 1 DS-GVO?" reicht dem formalen Akt, dass ein Dokument den Titel „Sicherheitskonzept" trägt. Die fachlich versierte Prüfung verlangt zusätzlich, dass der Inhalt fachlich überzeugend ist.

Es gibt gute Gründe Beratung und Überwachung auch personell zu trennen, auch wenn Art. 39 DS-GVO die Ausführung beider Aufgaben durch dieselbe Person zulässt oder auch nahelegt. Eine erfolgreiche Beratung bedingt immer auch ein Vertrauensverhältnis des DSB zu den handelnden Personen aus den Fachbereichen. Im Vordergrund steht, gemeinsam eine Lösung zu entwickeln. Im Idealfall agiert der DSB auf Augenhöhe des Fachbereichs. Eine Prüfungssituation ist dagegen durch eine Machtasymmetrie zu Gunsten des Prüfers gekennzeichnet. Diese Machtasymmetrie verträgt sich nicht unbedingt gut mit einer Beratung auf Augenhöhe („Alles was ich in der Beratung sage, wird in der Prüfung gegen mich verwendet."). Deshalb ist es empfehlenswert, dass die Überwachung von einer anderen Person durchgeführt wird, die nicht an der Beratung beteiligt war.

Prüfungszeiträume festlegen

Als letzten Schritt werden die geplanten Prüfungen zeitlich verteilt. Dabei sollte berücksichtigt werden, dass jede Prüfung neben der Durchführung auch einer Vorbereitung und einer Berichterstellung bedarf. Die Verfügbarkeit des Prüfers sollte berücksichtigt werden.

IV. Durchführung der Prüfung

Die Durchführung der Prüfung bedarf weiterer Aktivitäten.

Prüfungsvorbereitung

Wie soll der im Überwachungsplan festgelegte Gegenstand geprüft werden? Die Prüfungsmethodik, z. B. Interview, Überprüfung von Kontrolldokumenten, Sichtprüfung in Systemen, ist auszuwählen. Die verschiedenen Methoden unterscheiden sich hinsichtlich ihrer Aufwände und der erreichten Prüftiefe. Auch hier hilft eine Risikobetrachtung weiter. Gehen vom Prüfgegenstand geringe Risiken aus, ist eine Methode mit geringer Prüftiefe und geringem Aufwand vertretbar. Ein Beispiel wäre, sich durch die zuständigen Personen bestätigen zu lassen, dass die zu prüfenden Regeln eingehalten werden. Bei hohen Risiken wäre beispielsweise eine eigene Sichtprüfung im System risikoangemessen.

Basierend auf der Methode bietet es sich an, einen Prüfbogen mit den durchzuführenden Prüfhandlungen zu erstellen. Dadurch wird sichergestellt, dass keine Prüfhandlung vergessen wird und er dient gleichzeitig der Dokumentation der Ergebnisse. Die folgenden Stichworte sollen einen Eindruck vermitteln, welche Prüfhandlungen je nach Prüfungsgegenstand denkbar sind:

- **Struktur und Verantwortlichkeit im Unternehmen**
  - Legt die Datenschutz-Policy Verantwortlichkeiten eindeutig fest?
  - Wie wird ein Bewusstsein über Datenschutzrisiken geschaffen?
- **Transparenz der Verarbeitung**
  - Haben Sie ein Verfahren implementiert, um Betroffenenanfragen innerhalb der gesetzlichen Frist zu bearbeiten?
  - Wie wurden alle Betroffenengruppen über die Datenerhebung informiert?
  - Wurde ein Prozess für Datenübertragbarkeit implementiert?
- **Rechtmäßigkeit der Verarbeitung**
  - Kann die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nachgewiesen werden?
  - Liegen Einwilligungen vor?
- **Verletzungen des Schutzes personenbezogener Daten**
  - Ist sichergestellt, dass Datenschutzverletzungen im Unternehmen erkannt und behandelt werden?
  - Haben Sie einen Notfallplan aufgestellt?

Die Stichprobengröße ist neben der Methode die zweite Stellschraube für die Prüftiefe. Größere Stichproben erhöhen Aufwand und Prüftiefe. Neben dem Umfang der Stichprobe ist auch das Verfahren zur Auswahl festzulegen. Sollen z. B. Personalakten überprüft werden, sind ganz verschiedene Auswahlmethoden denkbar. Aus der Mitarbeiterliste werden zufällig zehn Namen ausgewählt, deren Personalakten geprüft werden. Die Prüfung könnte sich aber auch auf alle BEM-Teilnehmer konzentrieren, wenn u. a. überprüft werden soll, dass BEM-Unterlagen nicht auch in der Personalakte abgelegt wurden.

Mit den betroffenen Fachbereichen sollten die Prüftermine vereinbart werden.

Prüfungsdurchführung

Zu den vereinbarten Terminen erscheint der Prüfer und führt die in seinem Prüfbogen festgelegten Prüfhandlungen durch, die eine Mitwirkung des Fachbereichs bedürfen. Die übrigen Prüfhandlungen kann er vorher oder nachher vollziehen. Wichtig ist, für jede Prüfhandlung das Ergebnis zu dokumentieren. Wenn die Vorgabe nicht oder nicht vollständig erfüllt ist, sollte die Abweichung dokumentiert werden.

Abschlussbericht

Der Abschlussbericht setzt die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO mit Blick auf die Überwachungstätigkeit um. Es empfiehlt sich kurz Prüfgegenstand, Methodik, Stichprobengröße und -auswahl sowie das Ergebnis zu dokumentieren. Weil die eigentlichen Prüfhandlungen im Prüfbogen dokumentiert sind, reicht im Abschlussbericht eine Zusammenfassung und Darstellung der Abweichungen. Wie Abweichungen behoben werden können, ist eine Beratungsfrage. Im Abschlussbericht sind deshalb keine Lösungsvorschläge zu unterbreiten.

Der Abschlussbericht sollte den überwachten Fachbereichen sowie der obersten Unternehmensleitung übergeben werden. Ob und welche weiteren Empfänger berücksichtigt werden sollen, sollte im Vorfeld abgestimmt werden.

Follow-up Aktivitäten

Wenn in der Überwachung Abweichungen festgestellt wurden, liegt es nahe, dass die Abweichungen behoben werden sollten. Für die Entscheidung über und Umsetzung der Maßnahmen ist der Verantwortliche zuständig. Der DSB schlüpft wieder in seine Beraterrolle und unterstützt den Verantwortlichen.

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.).

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

UMGANG MIT DATENPANNEN: ERFÜLLUNG VON MELDE- UND BENACHRICHTIGUNGSPFLICHTEN NACH DER DS-GVO

Dr. Henrik Hanßen

Sicherheitsvorfälle gehören mittlerweile unvermeidlich zum Unternehmensalltag und bestimmen immer häufiger auch die Schlagzeilen. Konnten solche Vorfälle oftmals noch unternehmensintern gehandhabt werden, wurden durch die Datenschutz-Grundverordnung (DS-GVO) strenge Pflichten zur Meldung von Verletzungen des Schutzes personenbezogener Daten (bzw. „Datenpannen") an Aufsichtsbehörden eingeführt. Daneben können Unternehmen verpflichtet sein, die von einer Datenpanne betroffenen Personen wie etwa Kunden oder Geschäftspartner über den Vorfall zu benachrichtigen. Der Verschärfung der Meldepflichten entsprechend haben die Aufsichtsbehörden seit Mai 2018 einen starken Anstieg der Meldungen von Datenpannen verzeichnet. Gleichzeitig zeigt sich aber auch, dass Unternehmen die Anforderungen der DS-GVO oftmals noch nicht effektiv in ihren Prozessen zur Reaktion auf Datenpannen berücksichtigt haben. Allerdings birgt ein nachlässiger Umgang mit Datenpannen nicht nur PR-Risiken, vielmehr können Verstöße gegen die Melde- und Benachrichtigungspflichten mit hohen Bußgeldern geahndet werden. Unternehmen sollten daher sicherstellen, dass sie ihren Pflichten im Ernstfall schnell und rechtskonform nachkommen können. Dieser Beitrag gibt einen Überblick über die relevanten Pflichten sowie Hinweise zur praktischen Umsetzung.

I. Verletzung des Schutzes personenbezogener Daten

Die nach der DS-GVO vorgeschriebenen Melde- und Benachrichtigungspflichten werden durch so genannte Verletzungen des Schutzes personenbezogener Daten ausgelöst. Darunter ist jede Verletzung der Sicherheit zu verstehen, die zur Vernichtung, Veränderung, unbefugten Offenlegung, zum Verlust oder unbefugten Zugang zu personenbezogenen Daten führt, die von dem Verantwortlichen, d. h. dem für die Verarbeitung verantwortlichem Unternehmen verarbeitet wurden (vgl. Art. 4 Nr. 12 DS-GVO). Es ist unerheblich, ob die Verletzung beabsichtigt oder bewusst herbeigeführt wurde oder ob sie auf einem unrechtmäßigen Verhalten beruht. Beispiele sind der Verlust oder Diebstahl von Datenträgern, eine versehentliche Datenlöschung, die irrtümliche Versendung von E-Mails an falsche Empfänger, ein unberechtigte Da-

tenzugriff durch einen Hacking-Angriff oder ein temporärer Entzug des Datenzugriffs durch eine Ransomware-Attacke (Krypto-/Erpressungstrojaner).

Abzugrenzen sind die nach der DS-GVO relevanten Datenpannen von anderen Sicherheitsverletzungen, die keine personenbezogenen Daten betreffen. Für letztere Fälle können sich Meldepflichten allerdings aus anderen Rechtsgrundlagen ergeben, z. B. wenn es sich bei dem betroffenen Unternehmen um einen so genannten. Anbieter digitaler Dienste oder den Betreiber einer so genannten kritischen Infrastruktur handelt.

II. Meldung an die Aufsichtsbehörde

1. Bestehen einer Meldepflicht

Liegt eine Verletzung des Schutzes personenbezogenen Daten vor, soll diese nach dem Willen des Gesetzgebers grundsätzlich an die zuständige Aufsichtsbehörde gemeldet werden (Art. 33 Abs. 1 S. 1 DS-GVO). Dies ist die Aufsichtsbehörde desjenigen Bundeslandes (bzw. bei Unternehmen mit mehreren Niederlassungen in der EU des Mitgliedsstaates), in dem das betroffene Unternehmen seine Hauptniederlassung hat.

Da dieser Grundsatz zu einer nicht mehr zu bewältigenden Zahl von Meldungen führen würde, sieht Art. 33 Abs. 1 S. 1, Hs. 2 DS-GVO eine Ausnahmeregelung mit erheblicher praktischer Bedeutung vor. Danach besteht keine Meldepflicht, soweit die Verletzung voraussichtlich zu keinem bzw. nur geringfügigem Risiko für die betroffenen Personen führt. Bei der Entscheidung für oder gegen eine Meldung müssen Unternehmen also eine Prognose der Risiken für die betroffenen Personen vornehmen, wobei ihnen ein – behördlich und gerichtlich überprüfbarer – Einschätzungsspielraum eingeräumt ist.

Bei dieser Prognose sind alle physischen, materiellen oder immateriellen Schäden für die betroffenen natürlichen Personen zu berücksichtigen, wie z. B. der Verlust der Kontrolle über personenbezogenen Daten, Diskriminierungen, Identitätsdiebstahl oder -missbrauch, finanzielle Verluste, Rufschädigungen oder sogar gesundheitliche Schäden. Ausgehend von den im Einzelfall in Betracht kommenden Schäden ist mittels der etablierten Risikoformel „Eintrittswahrscheinlichkeit x Schwere der Schäden" die Höhe des Risikos zu bewerten. Bei dieser Bewertung gilt es eine ganze Reihe von Faktoren zu berücksichtigen, wie z.B.:

- die Art der Verletzung (eine Verletzung der Vertraulichkeit von Daten wiegt z. B. schwerer als deren temporär eingeschränkte Verfügbarkeit),
- die Art, Sensitivität, Umfang und Anzahl der betroffenen Datensätze (z. B. wiegt die Betroffenheit von Gesundheitsdaten oder einer hohen Anzahl von Datensätzen grundsätzlich schwer),
- die Tragweite der Folgen für die von den Daten betroffenen Personen (drohende finanzielle Verluste wiegen z. B. schwer; umgekehrt kann die Verfügbarkeit von Backups bei einer Ransomware-Attacke das Risiko reduzieren),
- die Zahl der betroffenen Personen (je größer die Zahl der Betroffenen, desto höher ist regelmäßig das Risiko) oder
- Möglichkeiten zur Identifizierung der Betroffenen (z. B. eine dem Stand der Technik entsprechende und nicht kompromittierte Verschlüsselung bedeutet häufig nur ein geringfügiges Risiko für die Betroffenen).

Die Aufsichtsbehörden empfehlen, im Zweifel eine Meldung vorzunehmen. In Grenzfällen kann die Möglichkeit einer (telefonischen) Vorabmeldung erwogen werden, um eine erste behördliche Einschätzung zu erlangen.

2. Frist, Inhalt und Form

Eine Meldung an die Aufsichtsbehörde muss unverzüglich – d. h. so schnell wie möglich – und möglichst binnen 72 Stunden erfolgen. Diese Frist beginnt allerdings erst, sobald dem Unternehmen mit hinreichender Sicherheit bekannt geworden ist, dass eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist. Ist die Datenpanne bei einem Dienstleister/Auftragsverarbeiter aufgetreten, erfordert eine Kenntnisnahme eine entsprechende vorherige Information durch den Auftragsverarbeiter.

Im Einzelnen muss eine Meldung mindestens die folgenden Informationen enthalten (Art. 33 Abs. 3 DS-GVO): ▸

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und ungefähren Zahl der betroffenen Personen sowie der Kategorien und ungefähren Zahl der betroffenen Datensätze;
- Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- Beschreibung der wahrscheinlichen Folgen der Verletzung;
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Dem Verantwortlichen steht es frei, weitere Angaben zu machen, wie z. B. dazu, dass die Verletzung bei einem Dienstleister/Auftragsarbeiter eingetreten ist. Die Aufsichtsbehörde kann die Mitteilung weiterer Informationen fordern oder durch Verwaltungsakt anordnen.

Sollte es nicht möglich sein, innerhalb der 72-Stunden-Frist alle notwendigen Informationen zusammenzutragen, dürfen diese schrittweise gemeldet werden. Eine Nichteinhaltung der Frist ist zu begründen (Art. 33 Abs. 1 S. 2 DS-GVO).

Bestimmte Anforderungen an die Form stellt die DS-GVO nicht auf, sodass auch telefonische Meldungen denkbar sind. Die flexibelste und sicherste Möglichkeit zur Meldung stellt allerdings regelmäßig die Nutzung der von den Aufsichtsbehörden zur Verfügung gestellten Formulare dar. Für eine Übersicht der verfügbaren Formulare und Kontaktinformationen siehe

http://hoganlovells-blog.de/2018/07/30/meldung-von-datenpannen-nach-der-dsgvo-meldeformulare-der-aufsichtsbehoerden/

III. Benachrichtigung der Betroffenen

1. Bestehen einer Benachrichtigungspflicht

Eine Pflicht zur Benachrichtigung der betroffenen Personen besteht, wenn die Datenpanne ein hohes Risiko für die Betroffenen bewirkt. Die Höhe des Risikos ist nach den oben genannten Faktoren zu bestimmen (siehe II. 1.). Ein hohes Risiko kann z. B. vorliegen, wenn Dritte durch einen Hacking-Angriff Zugriff auf Datensätze mit Kundendaten erlangt haben oder wenn sensible Finanzinformationen an einen falschen Empfänger versendet wurden. Es ist zudem möglich, dass die Aufsichtsbehörde nach einer erfolgten Meldung die Benachrichtigung der betroffenen Personen durch Verwaltungsakt anordnet (Art. 58 Abs. 2 lit. e und Art. 34 Abs. 4 DS-GVO).

Die Plicht zur individuellen Benachrichtigung der Betroffenen kann in einigen Ausnahmefällen entfallen, soweit:

- der Verantwortliche zuvor geeignete Sicherheitsvorkehrungen getroffen hat (Art. 34 Abs. 3 lit. a) DS-GVO), wie insbesondere eine dem Stand der Technik entsprechende Verschlüsselung der Daten;
- der Verantwortliche durch nachträgliche Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach kein hohes Risiko für die Betroffenen mehr besteht (Art. 34 Abs. 3 lit.b) DS-GVO), z. B. durch umgehenden Austausch von entwendeten Zugangsdaten oder Fernlöschung von Daten auf einem verlorengegangenen Notebook oder
- durch die Benachrichtigung Informationen offenbart würden, die geheim gehalten werden müssen. Dies gilt aber nur, soweit die Interessen der betroffenen Personen an einer Benachrichtigung dieses Geheimhaltungsinteresse nicht überwiegen (§ 29 BDSG).

Oftmals weniger attraktiv ist eine weitere Ausnahme (Art. 34 Abs. 3 lit. c) DS-GVO): Der Verantwortliche kann von einer individuellen Benachrichtigung absehen, wenn dies einen unverhältnismäßigen Aufwand bedeutete, z. B. wegen der zeit- und ressourcenaufwändigen Ermittlung der Kontaktdaten der Betroffenen. In diesen Fällen fordern die Aufsichtsbehörden jedoch ersatzweise eine öffentliche Kommunikation der Datenschutzverletzung, z. B. durch eine Pressemitteilung im Internet.

2. Frist, Inhalt und Form

Die Benachrichtigung der Betroffenen muss unverzüglich erfolgen. Eine in Stunden festgelegte Frist existiert anders als bei der Meldepflicht nicht. Die Benachrichtigung ist in einer für den betroffenen Empfängerkreis einfachen und

leicht verständlichen Sprache zu verfassen. Sie muss mit Ausnahme der Angabe der Art der Datenpanne die gleichen Informationen enthalten, die auch bei einer Meldung an die Behörde erforderlich sind. Hierbei ist durchaus Fingerspitzengefühl gefragt, um nicht die Geltendmachung von Haftungsansprüchen durch Betroffene zu provozieren.

IV. Dokumentation

Unabhängig davon, ob eine Melde- oder Benachrichtigungspflicht besteht, müssen Verantwortliche alle im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten stehenden Fakten dokumentieren, einschließlich ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen (Art. 33 Abs. 5 DS-GVO). Auf diese Weise soll den Aufsichtsbehörden eine Grundlage für die Überprüfung der Einhaltung der Meldepflicht gegeben werden.

Abgesehen von der gesetzlichen Pflicht zur Dokumentation sollten Unternehmen Datenpannen auch deshalb umfassend analysieren und dokumentieren, um interne Sicherheitslücken aufzudecken, eine Grundlage für die Abwehr möglicher Haftungsansprüche von Betroffenen zu schaffen und/oder mögliche Regressansprüche gegen Verursacher der Datenpanne vorzubereiten. Ab einer gewissen Unternehmensgröße lohnt sich die Erstellung und Führung eines Verzeichnisses über aufgetretene Datenpannen, wie es Telekommunikationsdienstleister sogar schon nach altem Recht verpflichtend vorhalten müssen (vgl. § 109a Abs. 3 TKG).

V. Rechtsfolgen bei Verstößen

Verstöße gegen die Melde- und Benachrichtigungspflichten können als Ordnungswidrigkeit mit Geldbußen bis zu 10 Mio. Euro oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes verfolgt werden (Art. 83 Abs. 4 lit. a) DS-GVO). Die Nichtbeachtung von Anordnungen von Aufsichtsbehörden, wie etwa die Anordnung zur Benachrichtigung der Betroffenen, kann mit Bußgeldern bis zu 20 Mio. Euro oder 4 % des gesamten weltweit erzielten Jahresumsatzes sanktioniert werden. Im Streitfall trägt das Unternehmen jedenfalls das Risiko, die Richtigkeit seiner Prognoseentscheidung darlegen und beweisen zu müssen, wobei hierfür ex ante auf den Zeitpunkt der Entscheidung abzustellen ist.

VI. Handlungsempfehlungen

Unternehmen ist zu empfehlen, die Anforderungen der DS-GVO in ihren Data Breach Response Prozessen und zugehörigen Reaktionsplänen und Richtlinien zu berücksichtigen und diese nötigenfalls anzupassen. Hierbei sollten insbesondere die folgenden Aspekte berücksichtigt werden:

- ***Erkennen von Datenpannen:*** Um sicherzustellen, dass Datenpannen überhaupt bekannt werden, sollten Mitarbeiter angewiesen werden, mögliche Sicherheitsverletzungen an ihre Vorgesetzten und/oder den Datenschutzbeauftragten zu melden. Eine Sensibilisierung für das Erkennen von Datenpannen kann durch Schulungen erreicht werden. In Lieferketten sind Dienstleister/Auftragsverarbeiter vertraglich zur Mitteilung von Datenschutzverletzungen zu verpflichten.
- ***Einleitung von Gegenmaßnahmen:*** Gegenmaßnahmen sollten so früh wie möglich angestoßen werden, um den Sicherheitsvorfall zu beseitigen und seine Folgen abzumindern. Idealerweise sind geeignete Gegenmaßnahmen für typische Arten von Vorfällen im Reaktionsplan bereits definiert.
- ***Prüfung und Risikobewertung:*** Zudem sollte eine unverzügliche rechtliche Prüfung der Datenpanne sichergestellt sein, um einschlägige Pflichten zu ermitteln und eine Entscheidung für oder gegen eine Meldung und Benachrichtigung sowie ggf. weitere Maßnahmen zu treffen. In diesen Prozess sollte neben den relevanten Fachabteilungen, der Rechtsabteilung und des/der Datenschutzbeauftragten vor allem auch die Geschäftsführung frühestmöglich mit einbezogen werden.
- ***Festlegung der Kommunikationsstrategie:*** Sollte das Bestehen einer Melde- und Benachrichtigungspflicht festgestellt werden, bietet es sich an, eine Strategie für die Kommunikation des Vorfalls nach außen festzulegen.
- ***Meldung an Aufsichtsbehörde:*** Zur Sicherstellung der Einhaltung der ▸

Meldeplichten sollte ein Prozess zur Vornahme der fristgerechten und vollständigen Meldung des Vorfalls an die zuständigen Behörden festgelegt sein.

- ***Benachrichtigung der Betroffenen:*** Gleichermaßen sollte ein Ablaufplan für die Benachrichtigung der betroffenen Personen bestehen.
- ***Dokumentation:*** Ferner sollte sichergestellt sein, dass alle im Zusammenhang mit Datenpannen relevanten Fakten für Nachweiszwecke, zur internen Qualitätssicherung und Compliance festgehalten werden.
- ***Zuständigkeiten:*** Für alle genannten Maßnahmen müssen klare Rollen und Zuständigkeiten bestimmt sein, um die Reaktionsfähigkeit im Ernstfall sicherzustellen.
- ***Kontinuierliche Verbesserung:*** Im Sinne eines „Plan-Do-Check-Act“ Zyklus sollte die Funktionsfähigkeit der Maßnahmen idealerweise durch Probeabläufe geprüft und zudem nach den gewonnenen Erkenntnissen aus Ernstfällen laufend ergänzt und verbessert werden.

Über den Autor

Dr. Henrik Hanßen
ist Rechtsanwalt und Senior Associate bei Hogan Lovells am Standort Hamburg und berät internationale und deutsche Unternehmen zu allen Aspekten des Datenschutzrechtes und im IT-Recht.

▶ https://www.hoganlovells.com/de-de

▶ http://hoganlovells-blog.de/

Hogan Lovells

Anzeige

PFLICHT ZUR BENENNUNG EINES DATENSCHUTZBEAUFTRAGTEN UND ZUM FÜHREN EINES VERZEICHNISSES VON VERARBEITUNGSTÄTIGKEITEN IN DER ARZTPRAXIS

Prof. Dr. Thomas Hoeren

I. Einführung

Mit der Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union gilt seit dem 25. Mai 2018 ein neuer Rechtsrahmen für die Verarbeitung von personenbezogenen Daten innerhalb der EU. Zeitgleich hat der deutsche Gesetzgeber die nationale Rechtslage an die neue Verordnung angepasst und von den vorhandenen Öffnungsklauseln Gebrauch gemacht. Zum umfassenden Pflichtenprogramm nach der DS-GVO gehören u. a. die Benennung eines Datenschutzbeauftragten und das Führen eines Verzeichnisses von Verarbeitungstätigkeiten durch datenverarbeitende Stellen.

Die Verarbeitung von Gesundheitsdaten ist aufgrund der sensiblen Informationen über den Patienten besonders risikoreich. Angesichts der drastischen Bußgeldandrohungen durch die DS-GVO stellt sich daher gerade auch für Arztpraxen die Frage, ob sie den oben genannten Pflichten unterfallen. Diese Frage lässt sich aufgrund der vielfältigen Erscheinungsformen von Arztpraxen nicht pauschal beantworten. Zu unterscheiden ist zwischen Einzelpraxen und Gruppenpraxen. In der Einzelpraxis verfügt ein einzelner Arzt über angestellte Mitarbeiter (ggf. auch angestellte Ärzte). Bei Gruppenpraxen arbeiten entweder mehrere Ärzte mit gemeinsamen Patientenstamm zusammen (sog. Berufsausübungsgemeinschaften) oder die ärztliche Tätigkeit erfolgt getrennt bei gemeinsamer Nutzung bloßer organisatorischer Ressourcen (sog. Organisationsgemeinschaften).[1]

Zudem stellt das Datenschutzrecht unterschiedliche Anforderungen an öffentliche und nicht-öffentliche Stellen. Zwar ist das Betreiben einer ▸

[1] Dochow, PinG 2018, 51 (52).

Arztpraxis als öffentliche Stelle theoretisch denkbar. Im Regelfall sind Arztpraxen aber privatrechtliche Einrichtungen. Daher sind die Datenschutzvorgaben für nicht-öffentliche Stellen maßgeblich.

II. Benennung eines Datenschutzbeauftragten

Die Pflicht zur Benennung eines Datenschutzbeauftragten ist in Art. 37 DS-GVO geregelt. Dieser enthält im ersten Absatz eine Reihe von Tatbeständen, bei deren vorliegen in jedem Fall ein Datenschutzbeauftragter zu benennen ist. Daneben enthält Art. 37 Abs. 4 DS-GVO eine Öffnungsklausel für nationale Gesetzgeber, die es ermöglicht, auch in anderen als den genannten Fällen die Benennung eines Datenschutzbeauftragten vorzuschreiben. Der deutsche Gesetzgeber hat von dieser Öffnungsklausel für nicht-öffentliche Stellen in § 38 BDSG Gebrauch gemacht und damit die Pflicht zur Benennung eines Datenschutzbeauftragten erweitert.

1. Verpflichtende Benennung nach § 38 Abs. 1 S. 1 BDSG

Nach § 38 Abs. 1 S. 1 BDSG haben Verantwortliche einen Datenschutzbeauftragten zu benennen, „soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen". Diese Regelung gilt auch für Arztpraxen unabhängig von ihrer Organisationsform.

Zunächst erfordert § 38 Abs. 1 S. 1 BDSG, dass es sich um eine „automatisierte Verarbeitung" personenbezogener Daten handelt. Gemeint ist damit unter anderem jede IT-gestützte Datenverarbeitung.[2] In modernen Arztpraxen dürfte dieses Tatbestandsmerkmal regelmäßig erfüllt sein. Eine rein analoge Verwaltung von Patientendaten, Terminen und Abrechnungsfragen scheint in der heutigen Zeit kaum noch denkbar.

Darüber hinaus ist eine Pflicht nur dann anzunehmen, wenn „in der Regel mindestens zehn Personen ständig" mit der Datenverarbeitung beschäftigt sind. Diese Formulierung wirft einige Fragen auf. Weitgehend klar ist, dass die relevanten Stellen zumindest auf eine gewisse Dauer angelegt sein müssen.[3] Die konkrete Besetzung ist unerheblich. Auch freie Mitarbeiter oder Leiharbeitnehmer sind in die Berechnung einzubeziehen, ebenso wie Teilzeitbeschäftigte, Auszubildende, Volontäre und Praktikanten.[4]

Wichtig ist außerdem, dass die Datenverarbeitung zumindest auch fester Bestandteil des Aufgabenkreises der Mitarbeiter ist.[5] In einer ärztlichen Praxis dürften somit etwa Putzkräfte oder Hausmeister nicht in den relevanten Personenkreis fallen. Zwar hätten diese theoretisch die Möglichkeit, von entsprechenden personenbezogenen Daten Kenntnis zu erlangen. Die Datenverarbeitung ist jedoch – anders als beispielweise bei Sprechstundenhilfen – nicht Bestandteil ihrer Aufgabenkreise.

Umstritten ist schließlich, ob der Praxisinhaber, in den meisten Fällen also der Arzt selbst, bei der Zählung der Beschäftigten mit einbezogen werden muss. In der Literatur wird dies mit dem Verweis auf den Wortlaut von § 38 Abs. 1 S. 1 BDSG überwiegend abgelehnt.[6] Dort heißt es, dass Verantwortliche einen Datenschutzbeauftragten benennen müssen, soweit sie mehr als zehn Personen „beschäftigen". Der Praxisinhaber ist dabei der Verantwortliche; er ist „Beschäftigender" und nicht selbst Beschäftigter.

Damit lässt sich im Ergebnis festhalten, dass nach § 38 Abs. 1 S. 1 BDSG eine Benennungspflicht immer dann besteht, wenn die relevante Personenzahl von zehn Beschäftigten überschritten wird. Während dies bei Einzelpraxen selten der Fall sein wird, ist dies bei überörtlichen Berufsausübungsgemeinschaften schon eher anzunehmen, da die Beschäftigten an mehreren Praxisstandorten lediglich einer verantwortlichen Stelle zuzurechnen sind.[7]

2. Verpflichtende Benennung nach Art. 37 DS-GVO

Auch direkt aus Art. 37 Abs. 1 DS-GVO kann sich für Ärzte eine Pflicht zur Benennung eines Datenschutzbeauftragen ergeben. Insbesondere Art. 37 Abs. 1 lit. c) DS-GVO ist in diesem Zusammenhang von hoher Relevanz, da Ärzte im Regelfall Gesundheitsdaten i.S.d. Art. 9 Abs. 1 DS-GVO verarbeiten. Nach § 37 Abs. 1 lit. c) DS-GVO greift nämlich die Benennungspflicht immer dann, wenn die Kerntätigkeit eines Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem.

[2] BeckOK DatenschutzR/Moos, § 38 BDSG Rn. 6.

[3] Paal/Pauly, § 38 BDSG Rn. 8.

[4] Kühling/Buchner/Kühling/Sackmann, § 38 BDSG Rn. 10.

[5] Dochow, PinG 2018, 51 (58).

[6] Dochow, PinG 2018, 51 (58); BeckOK DatenschutzR/Moos, § 38 BDSG Rn. 9.

[7] Dochow, PinG 2018, 51 (58).

Art. 9 DS-GVO besteht. Damit nennt die Vorschrift zwei zentrale Tatbestandsvoraussetzungen. Zum einen muss die Verarbeitung zur Kerntätigkeit des Verantwortlichen gehören; zum anderen muss die Verarbeitung selbst auch „umfangreich" sein.

Zunächst ist dementsprechend zu klären, ob die Verarbeitung von Gesundheitsdaten zur Kerntätigkeit eines jeden Arztes gehört oder ob auch hier eine Differenzierung geboten ist. Der Erwägungsgrund 97 der DS-GVO gibt zur Frage der Kerntätigkeit eine Leitlinie vor. Dort heißt es, dass sich die Kerntätigkeit des Verantwortlichen im privaten Sektor auf dessen Haupttätigkeiten bezieht und nicht auf die Verarbeitung von personenbezogenen Daten als Nebentätigkeit. Im medizinischen Sektor ist eine Kerntätigkeit damit zumindest dann anzunehmen, wenn das Geschäftsmodell eines Unternehmens auf der massenhaften Datenverarbeitung beruht, also etwa bei Laboren, die sich auf Genanalysen spezialisiert haben.[8] Im Falle von „gewöhnlichen" Ärzten wird teilweise argumentiert, die Verarbeitung von Gesundheitsdaten gehöre nicht zu deren Kerntätigkeit. Die ärztliche Profession lasse sich nicht auf eine reine Datenverarbeitung reduzieren.[9] Geschäftsmodelle von Ärzten seien keineswegs auf die Analyse von Patientendaten ausgerichtet. Vielmehr wurzelten sie in den kraft akademischer Ausbildung erlernten Fähigkeiten und geistigen Leistungen der Ärzte.

Dem wird allerdings zu Recht entgegengetreten. Die Hauptaufgabe der Ärzte ist die Behandlung von Patienten und die Bekämpfung von Krankheiten. Dies erfordert regelmäßig eine umfassende Untersuchung und Beobachtung des Patienten, typischerweise auch über einen längeren Zeitraum.[10] Ohne dabei beispielsweise in Krankenakten gesundheitsbezogene Daten der Patienten zu verarbeiten, wäre der Arzt kaum in der Lage, seiner Aufgabe in wirksamer Form nachzukommen.[11] Somit ist davon auszugehen, dass auch bei niedergelassenen Hausärzten die Verarbeitung von sensiblen Daten Teil der Kerntätigkeit ist.

Diese Datenverarbeitung muss allerdings nach Art. 37 Abs. 1 lit. c) DS-GVO auch „umfangreich" sein, damit sie die Pflicht zur Benennung eines Datenschutzbeauftragten begründen kann. Wann eine solche „umfangreiche" Verarbeitung anzunehmen ist, lässt sich der DS-GVO allerdings nicht direkt entnehmen. Lediglich Erwägungsgrund 91 der Verordnung befasst sich mit dem Begriff der umfangreichen Verarbeitung. Dabei ist allerdings zu beachten, dass sich der Erwägungsgrund eigentlich auf Art. 35 DS-GVO bezieht und sich nicht ausdrücklich mit den Kriterien des Art. 37 DS-GVO befasst. Trotzdem vermag er einen ersten Anhaltspunkt bei der Auslegung geben, da auch Art. 35 DS-GVO den Begriff der „umfangreichen Verarbeitung" nutzt und eine einheitliche Auslegung innerhalb der Verordnung nahe liegt. Nach dem Erwägungsgrund sind umfangreiche Verarbeitungsvorgänge unter anderem solche, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und – beispielsweise aufgrund ihrer Sensibilität – wahrscheinlich ein hohes Risiko mit sich bringen. Auch die Art. 29-Datenschutzgruppe schlägt für die Auslegung des Begriffs ähnliche Kriterien vor.[12]

Speziell in Bezug auf den medizinischen Sektor ist nach dem Erwägungsgrund nicht von einer umfangreichen Verarbeitung auszugehen, wenn die Verarbeitung personenbezogener Daten von Patienten durch einen einzelnen Arzt erfolgt. Dies legt nahe, dass das Kriterium der Beschäftigtenzahl bzw. die Zahl der Personen, die auf die Daten Zugriff haben, auch im Rahmen der Benennungspflicht nach der DS-GVO eine Rolle spielen mag. Gleichwohl sorgt aber auch dieser Hinweis nicht für die nötige Rechtssicherheit in der Praxis. Wann nämlich im positiven Sinne eine „umfangreiche Verarbeitung" und damit einhergehend eine Benennungspflicht anzunehmen ist, lässt sich dem Erwägungsgrund nicht entnehmen.

Teilweise wird bei der Frage nach einer „umfangreichen Verarbeitung" i.S.d. DS-GVO auch auf § 38 Abs. 1 BDSG verwiesen. Der Bundesgesetzgeber habe bei der Schaffung des § 38 Abs. 1 BDSG die Wertung nachvollzogen, dass eine „umfangreiche Verarbeitung" erst in Betracht kommt, wenn mindestens zehn Personen mit der Datenverarbeitung befasst seien.[13] Dieses Argument vermag jedoch nicht zu überzeugen. Die DS-GVO ist unabhängig vom ▸

[8] Dochow, PinG 2018, 51 (58).
[9] Dochow, PinG 2018, 51 (58).
[10] Kühling/Buchner/Bergt, Art. 37 DS-GVO Rn. 24.
[11] Art. 29-Datenschutzgruppe, WP 243, S. 8.
[12] Art. 29-Datenschutzgruppe, WP 243, S. 9.
[13] Dochow, PinG 2018, 51 (59).

Willen der nationalen Gesetzgeber auszulegen. Das Recht der nationalen Gesetzgeber zur Regelung der Benennungspflicht umfasst nur andere als die in Art. 37 Abs. 1 DS-GVO genannten Fälle, vgl. Art. 37 Abs. 4 DS-GVO.

Trotzdem sieht auch die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder eine Benennungspflicht für Ärzte vor, soweit diese in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen.[14] Dabei soll der Praxisinhaber selbst mitzuzählen sein. Wenn weniger als zehn Personen mit der Verarbeitung beschäftigt sind, soll in der Regel kein Datenschutzbeauftragter zu benennen sein. Eine Ausnahme davon sei zu machen, wenn im Einzelfall ein hohes Risiko für Rechte und Freiheiten zu erwarten ist.

Wenngleich diese Hinweise der Aufsichtsbehörden vor dem Hintergrund der Rechtssicherheit zu begrüßen sind, so findet die pauschale Festlegung einer relevanten Personenanzahl in der DS-GVO selbst keinerlei Stütze. Vielmehr gebietet eine unionsrechtskonforme Auslegung eine umfassende Abwägung im Einzelfall anhand der oben genannten Kriterien. Bei Einzelpraxen dürfte diese Abwägung – schon wegen der ausdrücklichen Nennung in Erwägungsgrund 91 – regelmäßig dahingehend ausfallen, dass die Benennung eines Datenschutzbeauftragten nicht erforderlich ist.

III. Führen eines Verzeichnisses von Verarbeitungstätigkeit

In einem weiteren Schritt stellt sich die Frage, ob eine Arztpraxis ein „Verzeichnis von Verarbeitungstätigkeiten" führen muss, welches das nach altem Recht bekannte Verfahrensverzeichnis ersetzt. Ein solches Verzeichnis ist eine schriftliche oder elektronische Aufzeichnung aller Verarbeitungstätigkeiten mit personenbezogenen Daten.[15] Diese Auflistung ist vorzuhalten und gem. Art. 30 Abs. 4 DS-GVO der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Zur Erstellung und Führung eines solchen Verzeichnisses ist nach Art. 30 Abs. 1 DS-GVO jeder „Verantwortliche" verpflichtet. Verantwortlicher ist gem. Art. 4 Nr. 7 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern gilt die Pflicht zum Führen eines Verzeichnisses gem. Art. 30 Abs. 5 DS-GVO allerdings nicht, es sei denn, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gem. Art. 9 Abs. 1 DS-GVO.

Damit sind auch Arztpraxen zum Führen eines Verzeichnisses von Verarbeitungsvorgängen verpflichtet. Zum einen entscheiden Ärzte über die Verarbeitung von personenbezogenen Daten in ihrer Praxis und sind damit Verantwortliche i.S.d. Art. 4 Nr. 7 DS-GVO. Zum anderen werden in einer Arztpraxis regelmäßig besondere Kategorien personenbezogener Daten verarbeitet, zu denen nach Art. 9 Abs. 1 DS-GVO auch Gesundheitsdaten gehören.[16] Wie ein solches Verzeichnis für eine Arztpraxis aussehen könnte, hat das Bayerische Landesamt für Datenschutzaufsicht in einem Muster beispielhaft dargestellt.[17]

IV. Fazit

Die Frage nach der Pflicht zur Benennung eines Datenschutzbeauftragten ist für Arztpraxen differenziert zu beantworten. Unproblematisch besteht eine solche Pflicht aus § 38 Abs. 1 S. 1 BDSG nur, wenn ein Arzt in seiner Praxis mindestens zehn Mitarbeiter mit der Datenverarbeitung beschäftigt. Gerade für Arztpraxen mit weniger als zehn Mitarbeitern ist allerdings vieles streitig. Hingegen besteht für sämtliche Arztpraxen die Pflicht zum Führen eines Verzeichnisses von Verarbeitungsvorgängen. Diese Pflicht besteht insbesondere unabhängig von der Mitarbeiterzahl und verlangt nicht, dass die Datenverarbeitung zur Kerntätigkeit der Praxis gehört.

[14] Datenschutzkonferenz, Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/DSB-Bestellpflicht.pdf (zuletzt abgerufen am: 10.09.2018).

[15] Siehe allgemein zum Verzeichnis von Verarbeitungstätigkeiten: Datenschutzkonferenz, Kurzpapier Nr. 1 – Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO, abrufbar unter: https://www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf (zuletzt abgerufen am: 10.09.2018).

[16] Bundesärztekammer, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, S. 12, abrufbar unter: https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf (zuletzt abgerufen am: 10.09.2018).

[17] Bayerisches Landesamt für Datenschutzaufsicht, Muster 5: Arztpraxis – Verzeichnis von Verarbeitungstätigkeiten, abrufbar unter: https://www.lda.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf (zuletzt angerufen am: 10.09.2018).

V. Weiterführende Links

• *Bayerisches Landesamt für Datenschutzaufsicht*, Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc. – Muster 5: Arztpraxis, abrufbar unter:

https://www.lda.bayern.de/media/muster_5_arztpraxis.pdf

(zuletzt abgerufen am: 10.09.2018).

• *Bundesärztekammer*, Hinweise und Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, abrufbar unter:

https://www.bundesaerztekammer.de/fileadmin/user_upload/downloads/pdf-Ordner/Recht/Hinweise_und_Empfehlungen_aerztliche_Schweigepflicht_Datenschutz_Datenverarbeitung_09.03.2018.pdf

(zuletzt abgerufen am: 10.09.2018).

• *Datenschutzkonferenz*, Datenschutzbeauftragten-Bestellpflicht nach Artikel 37 Abs. 1 lit. C Datenschutz-Grundverordnung bei Arztpraxen, Apotheken, und sonstigen Angehörigen eines Gesundheitsberufs – Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder – Düsseldorf, 26. April 2018, abrufbar unter:

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/04/DSB-Bestellpflicht.pdf

(zuletzt abgerufen am: 10.09.2018).

• *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Die Datenschutz-Grundverordnung tritt in Kraft – das müssen selbstständige Heilberufler beachten, abrufbar unter:

https://www.datenschutzzentrum.de/artikel/1220-Die-Datenschutz-Grundverordnung-tritt-in-Kraft-das-muessen-selbstaendige-Heilberufler-beachten.html

(zuletzt abgerufen am: 10.09.2018).

Über den Autor

Prof. Dr. Thomas Hoeren

Rechtswissenschaftliche Fakultät
ITM – Institut für Informations-, Telekommunikations- und Medienrecht
- Landeskompetenzzentrum -
Zivilrechtliche Abteilung

▶ www.uni-muenster.de

Anzeige

Werden Sie jetzt DSGVO-konform!
GDPR

Die Software, die Ihnen hilft, den Datenschutz effizient zu managen.

Entwickelt von Datenschutzpraktikern für Datenschutzpraktiker bietet 2B Advice PrIME Ihnen alle notwendigen Datenschutzwerkzeuge aus einer Hand.

2B Advice PrIME
Einzelplatzlizenz jetzt kostenlos bestellen unter
https://www.2b-advice.com/prime

2B Advice PrIME ®

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Dokumentieren Sie die Verarbeitung Ihrer personenbezogenen Daten. Erheben Sie Verarbeitungen direkt online bei den Fachverantwortlichen und passen Sie die Eingabemaske individuell Ihrem Corporate Design an.

TOM DOKUMENTIEREN

Dokumentieren Sie Ihre technischen und organisatorischen Maßnahmen.
Nutzen Sie jetzt 2B Advice PrIME, um eine Datenschutzfolgenabschätzung nach der DSGVO durchzuführen.

SCHULUNGEN

Sensibilisieren Sie die Mitarbeiter Ihres Unternehmens für aktuelle Anforderungen von Datenschutz und Datensicherheit. Nutzen Sie dafür individuell erstellbare Trainings und Mustervorlagen.

PRÜFUNGEN

Überprüfen Sie Ihre Compliance, identifizieren Sie Schwachstellen im Datenschutz und beheben Sie diese durch regelmäßige Prüfungen.

KOSTENLOSER WEBCAST

An jedem letzten Freitag des Monats bieten wir Ihnen eine kostenlose Online-Schulung (14 -15 Uhr) an.
Anmeldung unter
https://www.2b-advice.com/prime

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

ÜBERGABE DER DOKUMENTATION BEI WECHSEL DES DATENSCHUTZBEAUFTRAGTEN IM UNTERNEHMEN – INSBESONDERE ÜBERGABE DES E-MAIL-POSTFACHES

Dr. Carlo Piltz

A. Einleitung

Scheidet ein Datenschutzbeauftragter aus einem Unternehmen aus, ist oft fraglich, wie man mit seinen Unterlagen verfahren soll. Die DS-GVO macht zu dieser Thematik keine spezifischen Vorgaben. Wunsch aller Parteien ist sicherlich, dem neuen Datenschutzbeauftragten Zugang zu der Dokumentation und auch laufenden Verfahren des ausgeschiedenen Datenschutzbeauftragten zu ermöglichen. Die Dokumentationsübergabe umfasst heutzutage natürlich auch die Übergabe des E-Mail-Postfaches. Doch wie ist bei einem Wechsel eines Datenschutzbeauftragten eine geordnete Übergabe der Dokumentation durchzuführen? Insbesondere in Fällen, in denen ein Datenschutzbeauftragter ein Unternehmen ungeplant oder gar im Streit verlässt, stellen sich Fragen nach einer geordneten Übergabe der Unterlagen und des E-Mail-Postfaches.

B. Erforderlichkeit einer Übergabe

Erfolgt eine ordnungsgemäße Übergabe der Dokumentation des ausscheidenden Datenschutzbeauftragten an den neuen Datenschutzbeauftragten nicht bzw. nicht rechtzeitig, läuft das Unternehmen Gefahr seinen gesetzlichen Pflichten, nicht nur gegenüber dem neuen Datenschutzbeauftragten, sondern auch gegenüber den Betroffenen, nicht gerecht werden zu können.

Die Rechtstellung des Datenschutzbeauftragten gemäß Art. 38 DS-GVO beinhaltet nämlich nicht nur die Berichts-, Beratungs- und Geheimhaltungspflichten des Datenschutzbeauftragten, sondern verpflichtet den Verantwortlichen bzw. den Auftragsverarbeiter gegenüber den Datenschutzbeauftragten zur rechtzeitigen Einbindung, Unterstützung und Gewährleistung der Unabhängigkeit.[1] Übergibt das Unternehmen das E-Mail-Postfach nicht bzw. nicht rechtzeitig an den neuen Datenschutzbeauftragten, beeinträchtigt dies die rechtszeitige Einbindung des neuen Datenschutzbeauftragten im Sinne des Art. 38 Abs. 1 DS-GVO.

Des Weiteren ist die ordnungsgemäße Übergabe der relevanten Unterlagen des ausscheidenden Datenschutzbeauftragten an den neuen Datenschutzbeauftragten für das Unternehmen deswegen von großer Bedeutung, weil das Unternehmen als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO zur Wahrung der Betroffenenrechte verpflichtet ist. Sollte sich allerdings herausstellen, dass sich im E-Mail-Postfach des ausgeschiedenen Datenschutzbeauftragten unter anderem Anfragen von betroffenen Personen befinden, deren Beantwortung noch aussteht, läuft das Unternehmen Gefahr, seiner Pflicht, die Betroffenenrechte zu wahren, nicht nachkommen zu können.

Fraglich ist allerdings zum einem, ob die Verschwiegenheitspflicht des Datenschutzbeauftragten (Art. 38 Abs. 5 DS-GVO) einer solchen Übergabe des E-Mail-Postfaches an den neuen Datenschutzbeauftragten nicht entgegensteht und zum anderen, welche Anforderungen an die Durchführung einer solchen Übergabe zu stellen sind, insbesondere, ob Betroffene der E-Mail-Postfach-Übergabe an den neuen Datenschutzbeauftragten zustimmen müssen.

[1] Klug, in: Gola DS-GVO, 2. Aufl. 2018, Art. 38 Rn. 1.

C. Steht die Schweigepflicht des Datenschutzbeauftragten der Übergabe entgegen?

Die Frage, ob die Tätigkeit des Datenschutzbeauftragten, im Rahmen derer er zur Verschwiegenheit verpflichtet ist, einer Übergabe seines E-Mail-Postfaches an den neuen Datenschutzbeauftragten entgegensteht, kann nach der hier vertretenen Auffassung verneint werden.

1. 7. Tätigkeitsbericht 2015/2016 des Bayerischen Landesamts für Datenschutzaufsicht

Im seinem 7. Tätigkeitsbericht 2015/2016[2] geht das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), freilich noch zur alten Rechtslage, zurecht davon aus, dass bei einem Wechsel des Datenschutzbeauftragten auf eine Übergabe der relevanten Unterlagen des bisherigen Datenschutzbeauftragten an den neuen Datenschutzbeauftragten zu achten ist, um im Interesse des Unternehmens und der von den Daten betroffenen Personen (Kunden, Mitarbeiter, Lieferanten etc.) eine möglichst reibungslose und effektive Weiterarbeit des neuen Datenschutzbeauftragten sicherzustellen sowie die Persönlichkeitsrechte der Betroffenen zu wahren.

Das BayLDA führt weiter aus, dass beispielsweise die (damals noch so genannten) Verfahrensverzeichnisse, Unterlagen über durchgeführte Vorabkontrollen, beim Datenschutzbeauftragten noch laufende Beschwerdefälle von Betroffenen sowie für die Zukunft noch relevante abgeschlossene Fälle zu übergeben sind. Gleiches gelte für die für das Unternehmen erstellten Tätigkeitsberichte, Materialien bzgl. Mitarbeiterschulungen und Unterlagen zu den organisatorischen Datenschutzregelungen des Datenschutzbeauftragten. Aus dem Tätigkeitsbericht geht hervor, dass das BayLDA von dem zu übergebenden Umfang auch laufende Beschwerde- und Beratungsanfragen umfasst sieht. Eine solche Übergabe ist faktisch nur durchführbar, wenn der neue Datenschutzbeauftragte auch Zugriff auf das Postfach des vorherigen Datenschutzbeauftragten erhält. Denn andernfalls könnte der neue Datenschutzbeauftragte keine Kenntnis darüber erlangen, ob und wenn ja,

welche aktuellen Beschwerde- und Beratungsanfragen bei dem Datenschutzbeauftragten liegen oder auch, ob und wie in der Vergangenheit Anfragen beantwortet worden sind.

In dem Beitrag im 7. Tätigkeitsbericht 2015/2016 geht das BayLDA dann jedoch weiter davon aus, dass *„vertraulich an die bestimmte Person des Datenschutzbeauftragten gerichtete Betroffenen-Anfragen bzw. Datenschutzbeschwerden (siehe § 4f Abs. 4 BDSG)“* vom bisherigen Datenschutzbeauftragten *„bei Erledigung grundsätzlich zu löschen oder zu vernichten“* sind und bei noch laufenden Fällen solcher vertraulicher Art *„durch Rückfrage beim Betroffenen zu klären“* ist, wie er sein Anliegen weiter behandelt haben möchte.

Verweigert der ehemalige Datenschutzbeauftragte in den in der Einleitung genannten Extremsituationen seine Mitarbeit an der Übergabe, stellt sich für das Unternehmen die Frage, wie das Unternehmen vorgehen sollte.

Nach der hier vertretenen Auffassung kann in diesem Fall auch der neue Datenschutzbeauftragte das bestehende E-Mail-Postfach des alten Datenschutzbeauftragten übernehmen ▸

[2] 7. Tätigkeitsbericht 2015/2016 des Bayrischen Landesamt für Datenschutzaufsicht (BayLDA), S. 36, abrufbar unter: https://www.lda.bayern.de/media/baylda_report_07.pdf.

und in diesem Zuge auch solche Verfahren zur Kenntnis nehmen, die der Verschwiegenheitspflicht des Datenschutzbeauftragten unterliegen, da der neue Datenschutzbeauftragte ansonsten nicht seinen Aufgaben nachkommen kann und zu befürchten ist, dass sich Anfragende zum Beispiel an eine Aufsichtsbehörde mit dem Argument wenden, dass sie auf ihre Beschwerde keine Antwort oder Rückmeldung erhalten.

Sowohl für den alten als auch den neuen Datenschutzbeauftragten gilt die gesetzliche Verschwiegenheitspflicht, weshalb auch bei einem Wechsel in der Person des Datenschutzbeauftragten die Rechte der Betroffenen gewahrt bleiben. Hiervon umfasst ist dann natürlich auch der Zugriff auf das bestehende E-Mail-Postfach des Datenschutzbeauftragten.

2. Parallele: Betriebsärztliche Verschwiegenheitspflicht nach § 3 Arbeitssicherheitsgesetz

Nach der hier vertretenen Auffassung könnte man zur Begründung auch auf die Übergabe von patientenbezogenen Unterlagen bei Betriebsärzten abstellen. Nach § 3 Arbeitssicherheitsgesetz (ASiG) ist es Aufgabe des Betriebsarztes, den Arbeitgeber beim Arbeitsschutz und bei der Unfallverhütung in allen Fragen des Gesundheitsschutzes zu beraten und zu unterstützen. Die Aufgaben sind daher mit jenen des Datenschutzbeauftragten im Datenschutzrecht zu vergleichen. Auch die betriebsärztliche Dokumentation beinhaltet arbeitnehmerbezogen individuelle medizinische wie auch arbeitgeber- bzw. unternehmens- und arbeitsplatzbezogene Aspekte. Auch unterliegt der Betriebsarzt der ärztlichen Schweigepflicht und hat nach § 8 Abs. 1 ArbSiG eine dem Arbeitgeber gegenüber unabhängige Stellung und auch diesem gegenüber die ärztliche Schweigepflicht zu wahren. Auch diese Schweigepflicht und die Stellung des Betriebsarztes ähneln der Verschwiegenheitspflicht des Datenschutzbeauftragten gegenüber dem Verantwortlichen oder Auftragsverarbeiter. Im 5. Tätigkeitsbericht 2011/2012[3] vergleicht auch das BayLDA die Handhabung von E-Mails an den Betriebsarzt mit jenen an den betrieblichen Datenschutzbeauftragten. Diese müssen dem Zugriff des Arbeitgebers entzogen bleiben, *„weil nur so diese Stellen die Vertraulichkeit wahren können, zu der sie verpflichtet sind"*.

Konkret zur Übergabe von Patientenakten des internen Betriebsarztes wird in den „Hinweisen zur datenschutzgerechten Übergabe einer Arztpraxis mit Patientenakten und zum Wechsel von Betriebsärzten"[4] des Unabhängigen Landeszentrums für Datenschutz (ULD) aus Schleswig-Holstein vom 10. Januar 2015 davon ausgegangen, dass bei einem Wechsel eines internen Betriebsarztes die patientenbezogenen Unterlagen zunächst im Besitz des Arbeitgebers verbleiben. Dieser darf aber, mit Blick auf die ärztliche Schweigepflicht, die weiter gilt, keinen Einblick in die Unterlagen nehmen. Der Arbeitsgeber hat sie vielmehr dem neu bestellten Betriebsarzt auszuhändigen. Aus Sicht des ULD ist die Zustimmung des Arbeitnehmers für die Übergabe der Dokumentation an den neuen Betriebsarzt nicht erforderlich. Aus Transparenzgründen seien die Mitarbeiter rechtzeitig und umfassend über den geplanten Wechsel des Betriebsarztes aufzuklären (z. B. durch Mitarbeiter-Rundschreiben). Dabei sei ihnen die Möglichkeit einzuräumen, Widerspruch gegen die Einsicht in patientenbezogene Informationen aus Vorsorgemaßnahmen zu erheben.

Für die hier gegebene Konstellation des Wechsels des Datenschutzbeauftragten könnten die Mitarbeiter informiert werden, denen die Möglichkeit eingeräumt werden soll, gegen die Übernahme von laufenden Anfragen oder Beschwerden an den Datenschutzbeauftragten, die der Verschwiegenheitspflicht unterliegen, Widerspruch zu erheben.

Jedoch könnte diese Lösung nicht gegenüber externen Betroffenen und ehemaligen Mitarbeiter angeboten werden, da der neue Datenschutzbeauftragte, ohne Einsicht in das E-Mail-Postfach, keine Kenntnis davon hat, ob Beschwerden von externen Personen vorhanden sind oder nicht und wer diese Personen sind. Das Unternehmen kann nicht wissen, welche Adressaten es kontaktieren muss, um auf die die Widerspruchsmöglichkeit hinzuweisen.

[3] Der 5. Tätigkeitsbericht 2011/2012 des Bayrischen Landesamt für Datenschutzaufsicht (BayLDA), S. 63f, abrufbar unter: https://www.lda.bayern.de/media/baylda_report_05.pdf.

[4] Hinweise zur datenschutzgerechten Übergabe einer Arztpraxis mit Patientenakten und zum Wechsel von Betriebsärzten sind die Webseite des ULD abrufbar über: https://www.datenschutzzentrum.de/artikel/47-Hinweise-zur-datenschutzgerechten-UEbergabe-einer-Arztpraxis-mit-Patientenakten-und-zum-Wechsel-von-Betriebsaerzten.html.

D. Schluss

Eine, der Verschwiegenheit unterliegende, Eröffnung der Zugriffsmöglichkeit auf das E-Mail-Postfach des Datenschutzbeauftragten durch den neuen Datenschutzbeauftragten ohne Einwilligung oder vorherigen Einräumung des Widerspruchs, kann daher für sinnvoll und begründbar erachtet werden. Zumindest in den Fällen, in denen es einem Unternehmen faktisch nicht möglich ist, die Betroffenen (z. B. Personen, die eine Beschwerde eingereicht haben) zu kontaktieren. Stellt der neue Datenschutzbeauftragte dann nach Sichtung der Unterlagen und Einsichtnahme in das E-Mail-Postfach fest, dass unbeantwortete Beschwerden oder noch nicht abgeschlossene Verfahren vorhanden sind, kann er sich direkt und gezielt an die Beschwerdeführer oder Anfragenden wenden. Die Rechte der Betroffenen werden durch diese Maßnahme nicht beschränkt, sondern vielmehr gewahrt, indem ihre Beschwerden (weiter)bearbeitet werden können.

Über den Autor

Dr. Carlo Piltz

Rechtsanwalt,
Reusch Rechtsanwaltsgesellschaft mbH, Berlin
Teamleader Cyber Security & Datenschutz
Zertifizierter Datenschutzbeauftragter (T.V.)
Certified Information Privacy Professional/Europe (CIPP/E)

▶ www.reuschlaw.de

reuschlaw
Legal Consultants

Anzeige

SECURITY BREACH NOTIFICATION – RISIKEN DER MELDEPFLICHT

Dr. Jens Eckhardt

Wenn es um die Meldung und Benachrichtigung von Verletzungen des Schutzes personenbezogener Daten geht müssen nicht nur die neu gestalteten Artt. 33, 34 DS-GVO sondern vor allem auch der insgesamt neu gestaltete Gesamtrahmen der DS-GVO ins Auge gefasst werden.

Der Beitrag beruht auf einem Vortrag im Rahmen der BvD-Herbstkonferenz am 25.10.2018 in Stuttgart.

Einführung: Warum es um mehr als nur Artt. 33, 34 DS-GVO geht!

Die Security Breach Notification wurde in Artt. 33, 34 DS-GVO im Vergleich zum BDSG-alt neu geregelt. Die Schwelle zur Meldung an die zuständige Datenschutzaufsichtsbehörde ist deutlich gesenkt worden.

Das ist aber nicht die einzige Veränderung, die bei einer Verletzung der Sicherheit personenbezogener Daten zu beachten ist. Wesentlich ist auch, dass erst seit der DS-GVO die Verletzung des Schutzes personenbezogener Daten, welche bisher die Hauptursache für Meldungen war, erstmals bußgeldbewehrt ist. Auch andere Pflichtverstöße sind erstmals bußgeldbewehrt. Auch könnten Benachrichtigungen unter der DS-GVO eher als unter dem BDSG-alt zu Schadensersatzansprüchen führen.

Pflicht zur Meldung und Benachrichtigung

Auslöser der Melde- und Benachrichtigungspflicht ist eine Verletzung des Schutzes personenbezogener Daten.

Wenngleich häufig eine IT-Sicherheitsverletzung die Grundlage einer Verletzung des Schutzes personenbezogener Daten ist, ist beides nicht gleichbedeutend. Auch kann eine Verletzung des Schutzes personenbezogener Daten in Betracht kommen, ohne dass eine IT-Sicherheitsverletzung gegeben ist. Auch hier zeigt sich – ebenso wie bei Art. 32 DS-GVO - der Unterschied zwischen IT-Sicherheit und Datenschutz, da beide Bereiche unterschiedliche Schutzziele haben.

Eine „Verletzung des Schutzes personenbezogener Daten“ ist nach Art. 4 Nr. 12 DS-GVO „eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“.

Es erfolgt – anders als nach § 42a BDSG-alt – keine Beschränkung auf bestimmte Datenkategorien. Auch ein Verschulden ist nicht Voraussetzung. Das bedeutet auch dann, wenn das Unternehmen nichts dafür kann, dass es zum Vorfall kam, besteht die Meldepflicht. Erforderlich ist allerdings die positive Kenntnis von dem Vorfall. Hier wird man sich aber in der Praxis vor dem Versuch hüten müssen, die Augen bewusst vor einem Vorfall verschließen zu wollen.

Des Weiteren ist ein Risiko bzw. ein hohes Risiko für die Rechte und Freiheiten der natürlichen Person nach Artt. 33, 34 DS-GVO erforderlich. Was ein Risiko ist, ist in der DS-GVO nicht explizit definiert. ErwGr. 59, 67 ff. DS-GVO enthalten Anhaltspunkte. Entscheidend ist, dass nach ErwGr. 76 S. 2 DS-GVO das Risiko objektiv zu bestimmen ist, womit es nicht auf die subjektive Sicht der einzelnen Person ankommt.

Die Art. 29 Gruppe hat in dem WP 250 rev.01 Anhaltspunkte für die Bewertung gegeben. Deutlich wird daran, dass die Bewertung im Rahmen von Artt. 33, 34 DS-GVO nicht zwingend deckungsgleich ist mit der Bewertung im Rahmen der Datenschutzfolgenabschätzung (DFSA) nach Art. 35 DS-GVO. Ein struktureller Unterschied besteht allein schon deshalb, weil

bei der DFSA eine Schadenswahrscheinlichkeit ein Aspekt der Bewertung ist, wohingegen diese Frage sich im Rahmen von Art. 33, 34 DS-GVO nicht mehr stellt, da sich die Wahrscheinlichkeit gerade realisiert hat.

Zwei wesentliche Unterschiede besteht zwischen der Meldepflicht gegenüber der Aufsichtsbehörde (Art. 33 DS-GVO) und der Benachrichtigung der betroffenen Person (Art. 34 DS-GVO):

- Die Meldepflicht nach Art. 33 DS-GVO besteht bei einem Risiko. Die Benachrichtigungspflicht besteht erst bei einem hohen Risiko.
- Das Regel-Ausnahme-Verhältnis ist ein anderes: Die Meldung nach Art. 33 DS-GVO ist der Regelfall und besteht nur dann nicht, wenn ein Risiko verneint wird („*... meldet ... es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt ...*"). Die Benachrichtigung ist nicht der Regelfall und besteht nur, wenn ein hohes Risiko besteht („*... voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt ...*").

Je nach Risiko steigt die Gefahr, dass sich ein Bußgeldverfahren oder eine Schadensersatzforderung anschließt. Neben der Risikoklassifizierung ist auch der Inhalt der Meldung entscheidend, wenn es darum geht, die Risiken eine Meldung und Benachrichtigung ins Auge zu fassen. In diesem Kontext ist folgender Inhalt der Benachrichtigungs- und Dokumentationspflicht hervorzuheben (Art. 33 Abs. 3 DS-GVO):

- Art der Verletzung des Schutzes personenbezogener Daten plus (soweit möglich) Kategorien und der ungefähren Zahl der betroffenen Personen, betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze (Abs. 3 lit. a)
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen (Abs. 3 lit. b)
- Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Abs. 3 lit. c)
- Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen (Abs. 3 lit. d).

Für die Benachrichtigung nach Art. 34 DS-GVO gilt: „*... beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Empfehlungen.*"

Warum ist dieser Inhalt so interessant, wenn es um die Risiken einer Meldung geht? Die Antwort ergibt sich durch einen Blick in Bußgeldzumessungskriterien nach Art. 83 Abs. 2 DS-GVO. Denn diese Inhalte sind auch wesentlich für die Bußgeldbemessung. Der Meldende liefert diese also „frei Haus". Ein Blick auf die Schadensersatzansprüche nach Art. 82 DS-GVO zeigt, dass mit der Benachrichtigung der betroffenen Person auch alle wesentlichen Inhalte zur Verfügung gestellt werden, die für eine Schadensersatzklage erforderlich sind.

Nicht übersehen werden darf, dass die Meldung und Benachrichtigung wie eine Art Geständnis wirkt und verwertet werden kann. Denn das Argument, das sei in der Meldung so ja nicht gemeint gewesen sein, wird wenig überzeugend sein. Darüber hinaus würde das Argument das Risiko des Vorwurfs des Verstoßes gegen Artt. 33, 34 DS-GVO bergen.

Eine Beratung zur Melde- und Benachrichtigungspflicht sollte daher auch über den Tellerrand der Artt. 33, 34 DS-GVO hinaus gehen. Denn der Veranwortliche könnte etwas irritiert reagieren, wenn ihm das erst bewusst gemacht wird, nachdem er gemeldet hat und womöglich glaubte, dass damit alles erledigt sei.

Nicht übersehen werden darf, dass die Meldung nach Art. 33 DS-GVO grundsätzlich binnen 72 Stunden erfolgen muss.

Wer ist zu Meldung und Benachrichtigung verpflichtet?

Nach Artt. 33, 34 DS-GVO ist der Verantwortliche zur Meldung verpflichtet. Damit ist zunächst klar, dass diese Pflicht nicht den Datenschutzbeauftragten originär trifft. In der Unternehmensorganisation ist mit Blick auf die in diesem Beitrag aufgezeigte Tragweite der (Nicht-)Meldung wichtig, dass im jeweiligen Unternehmen klar festgelegt ist, wer verantwortlich ist für die Entscheidung über die (Nicht-)Meldung. Aufgrund der damit unter Umständen auch verbundenen unternehmerischen Risikoentscheidung ist sinnvoll, diese bei der Unternehmensleitung anzusiedeln.

Das schließt es nicht aus, dass die Vorbereitung in einem in der Unternehmenshierarchie darunter angesiedelten Gremium vorbereitet wird. Die Rolle des Datenschutzbeauftragten besteht nach der DS-GVO zunächst in ▸

einer beratenden, aber nicht letztverantwortlich entscheidenden Funktion.

Die Aufgabe des Auftragsverarbeiters besteht nach Art. 33 Abs. 2 DS-GVO darin, dem Verantwortlichen – also den Auftraggeber – unverzüglich eine Verletzung des Schutzes personenbezogener Daten zu melden, wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird. Zivilrechtlich wird – vereinfacht gesagt – dem Auftraggeber typischerweise das Verhalten des Auftragnehmers zugerechnet, sodass der Auftraggeber ohnehin für das Verhalten seines Auftragnehmers haftet.

Auch in Konstellationen der Joint Controllership sollte festgelegt sein, wer meldet. Denn Verantwortlicher ist bei einer Joint Controllership – anders als bei der Auftragsverarbeitung – jeder Datenverarbeiter.

Auf den zweiten Blick: Möglichen Konsequenzen der (Nicht-)Meldung

Das rechtswidrige Unterlassen der Meldung und der Benachrichtigung ist jeweils 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, je nachdem, welcher der Beträge höher ist“*, belegt. Aus dieser Sanktion entspringt der Drang zur Meldung und Benachrichtigung. Darüber hinaus kann eine pflichtwidrig unterlassene Benachrichtigung der betroffenen Person Anknüpfungspunkt für einen Schadensersatzanspruch sein, wenn der Schaden (auch) auf die unterlassene Benachrichtigung zurück zu führen ist.

Diese Rechtslage darf – jedenfalls in der Beratung – nicht zur Blindheit für die Risiken führen. Die Meldung kann – wie bereits oben angesprochen – zu Bußgeldern und Schadensersatzansprüchen führen. Verdeutlichen Sie sich das:

Gegenstand der Meldung kann und wird häufig eine Verletzung einer anderen Pflicht der DS-GVO sein. Häufig wird es sich um eine Verletzung der Pflichten zur Sicherheit der Verarbeitung nach Art. 32 DS-GVO sein. Diese ist aber – wie praktisch alle Pflichten der DS-GVO – ihrerseits bußgeldbewehrt. Das bedeutet, dass häufig mit der Meldung ein bußgeldbewehrter Verstoß gestanden wird. Vergegenwärtigen Sie sich den umfangreichen Tatbestand des Art. 83 DS-GVO einmal aus dieser Perspektive.

Nach Art. 82 DS-GVO – und darüber hinaus auch aus einem eventuellen Vertrag und weiteren Anspruchsgrundlagen des Bürgerlichen Gesetzbuchs (BGB) – kommen Schadensersatzansprüche Betroffener in Betracht. Ob nur betroffenen Personen – also diejenigen, deren Daten verarbeitet wurden – oder weitere Personen danach anspruchsberechtigt sind, ist noch umstritten. Durch eine Benachrichtigung wird damit der Sachverhalt mitgeteilt, der zur Begründung einer Schadensersatzforderung erforderlich ist. Aufgrund von Art. 82 DS-GVO haften dafür dann auch die beteiligten Auftragsverarbeiter und Joint Controller. Der Schadensersatz ist nicht auf materielle Schäden beschränkt sondern umfasst auch immaterielle Schäden (Stichwort: Schmerzensgeld); wenngleich die deutsche Rechtsprechung bisher bei immateriellen Schäden zurückhaltend war, kann sich das unter der DS-GVO und der erforderlichen EU-weit einheitlichen Anwendung ändern.

Wirkt sich eine Meldung und Benachrichtigung bußgeldreduzierend aus? Art. 83 Abs. 2 sieht vor, dass bei der Bußgeldbemessung „jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens“ (Abs. 2 lit. c) und die „Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat“ (Abs. 2 lit. h) zu berücksichtigen ist. Diese Regelungen könnten so gehandhabt werden, dass die Erfüllung der Pflicht nach Artt. 33, 34 DS-GVO sowohl beim Ob als auch bei der Höhe zugunsten des Meldenden berücksichtigt werden. Sicherlich wird es aber auch Stimmen geben, die anführen, dass die Erfüllung einer ohnehin bestehenden gesetzlichen Pflicht (also Artt. 33, 34 DS-GVO) nicht auch noch belohnt werden darf.

Dann gibt es in §§ 42 Abs. 4, 43 Abs. 4 BDSG das sog. Beweisverwendungsverbot. Aber Vorsicht. Hierauf ist kein blinder Verlass (ausführlich Eckhardt/Menz DuD 2018, 139 ff.). Denn: Geschützt ist nur der Verantwortliche – also nicht die Geschäftsleitung und nicht der Handelnde, obwohl auch gegen diese Bußgelder in Betracht kommen. Darüber hinaus gibt es zu Parallelregelungen in anderen Gesetzen die Auslegung, dass nur das nicht verwendet werden, was die Behörde ohne die Meldung nicht selbst hätte ermitteln dürfen. Auch werden sich auch Stimmen finden, die argumentieren, dass dieses Beweisverwendungsverbot gegen die DS-GVO verstößt; was mit Blick auf deutsche verfassungsrechtliche Grundsätze und die Europäische Menschenrechtskonvention nicht so eindeutig ist. Selbst wenn zu hoffen bleibt, dass dieses Beweisverwendungsverbot großzügig ausgelegt wird, wird das erst die Praxis zeigen müssen. In der Bera-

tung sollte jedenfalls nicht „in blindem Vertrauen“ hierauf Bezug genommen werden.

Die Quintessenz

Die Melde- und Benachrichtigungspflicht ist im Sinne des Schutzes der betroffenen Person wichtig. Denn durch sie wird gerade dort durch Transparenz eine Schutzlücke geschlossen, wo sich die betroffene Person nicht selbst schützen kann. Denn sie wird eigenständig keine Kenntnis von der Verletzung der Sicherheit der personenbezogenen Daten erlangen können.

Andererseits ist die Melde- und Benachrichtigungspflicht für die Verpflichteten ein „hartes Los“; zumal wenn bedacht wird, dass diese Pflicht auch besteht, wenn der Verpflichtete nichts für den Vorfall kann. Es müssen bei der Meldung auch die möglichen Konsequenzen ins Auge gefasst werden. Um es platt zu sagen: Im Rahmen einer Meldung und Benachrichtigung darf nicht drauf los geplappert werden, sondern es muss in Abhängigkeit von der Wahrscheinlichkeit und Schwere der Konsequenzen die Meldung wohl überlegt gestaltet und auch begleitet werden.

Hart gesprochen, beginnt mit der Meldung und Benachrichtigung – jedenfalls ab einem gewissem Ausmaß der Ursache für die Meldung und Benachrichtigung – die Verteidigung gegen ein Bußgeld und Schadensersatzansprüche. Das darf keineswegs als Rat zur Nicht-Meldung missverstanden werden.

Aber sicherlich gilt wie folgt: Was immer Du tust, handle klug und bedenke das Ende!

Über den Autor

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

▶ www.derra.eu

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

"HUMAN FIREWALL"- WIE SIE MITARBEITER GEZIELT ZU CEO-FRAUD SENSIBILISIEREN

Stefan Bachmann

CEO-Fraud, CEO-Scam oder Fake-President-Fraud sind Bezeichnungen für eine Betrugsmasche, die auch für uns als Datenschutzbeauftragte ein wichtiges Sensibilisierungsthema sein kann. In Schulungen bieten diese Inhalte eine spannende Abwechslung mit hohem Mehrwert.

Was bedeutet CEO-Fraud?

Beim CEO-Fraud geben sich Täter als Geschäftsführer (CEO) oder Angestellte mit erweiterten Zahlungsbefugnissen aus und veranlassen einen Mitarbeiter zum Transfer eines größeren Geldbetrages ins Ausland.

Welche Unternehmen sind besonders betroffen?

Grundsätzlich findet man CEO-Fraud bei allen Unternehmensgrößen. Die Betrüger passen den Grund für die Überweisung und die Betrugssumme an die Unternehmensgröße an. Möchte man eine Hauptzielgruppe definieren, sind dies wohl kleine und mittlere Unternehmen. Im Gegensatz zu großen Firmen fehlen diesen meist strenge Kontrollmechanismen. Befindet man sich in einer starken Wachstumsphase, existieren meist noch größere Lücken in den Kontrollstandards.

Zusätzliche Herausforderungen ergeben sich mit Außenstandorten. Hier fehlt der direkte Bezug zu Mitarbeitern und Geschäftsleitung in der Firmenzentrale. Inhaltliche Fehler in der Wortwahl („Firmenslang") fallen in der Regel nicht auf.

Grundlage für einen erfolgreichen Angriff

Damit ein Angriff erfolgreich verlaufen kann, sind jegliche Informationen willkommen, die den Angreifer mit Insiderwissen ausstatten. Wirtschaftsberichte, Handelsregistereinträge, Organigramme, Vorträge, Werbebroschüren und Mitarbeiterkontaktdaten lassen sich sehr oft über die Webauftritte abgreifen. Weitere Details zu Funktion, Tätigkeit und private Interessen finden sich in sozialen Berufsnetzwerken. Eine Regel besagt: Fünf unwichtige Informationen ergeben eine zielführende.

Tatbegehung

Die Täter nehmen mit den „ausgeforschten" Mitarbeitern Kontakt auf und geben sich als leitende Angestellte, Geschäftsführer oder Handelspartner aus. Sehr oft wird dabei Mail-Spoofing eingesetzt, das Fälschen oder Verschleiern einer E-Mailadresse. Der Manipulationsversuch ist dabei aus dem Leben gegriffen. Steht ein Freund oder Bekannter vor der Tür, wird er unverzüglich gebeten einzutreten. Ein Fremder hingegen muss erst eine Fülle von Fragen über sich ergehen lassen, ehe ihm die Tür geöffnet wird.

Im E-Mailtext fordern die Betrüger den Transfer eines größeren Geldbetrages auf Konten in China und Hong Kong, aber auch in osteuropäischen Staaten. Als Gründe werden angebliche Unternehmensübernahmen oder geänderte Kontoverbindungen angegeben.

Welche Schäden können entstehen?

Die mir am höchsten bekannte Schadenssumme traf FACC im benachbarten Oberösterreich. Am 23. Dezember 2015 überwies ein Mitarbeiter der Finanzbuchhaltung die ersten 13 Millionen Euro an Internetbetrüger. 40 gefälschte E-Mails im Namen des Vorstandschefs Walter Stephan hatten ausgereicht das Unternehmen um 50 Millionen Euro zu prellen.

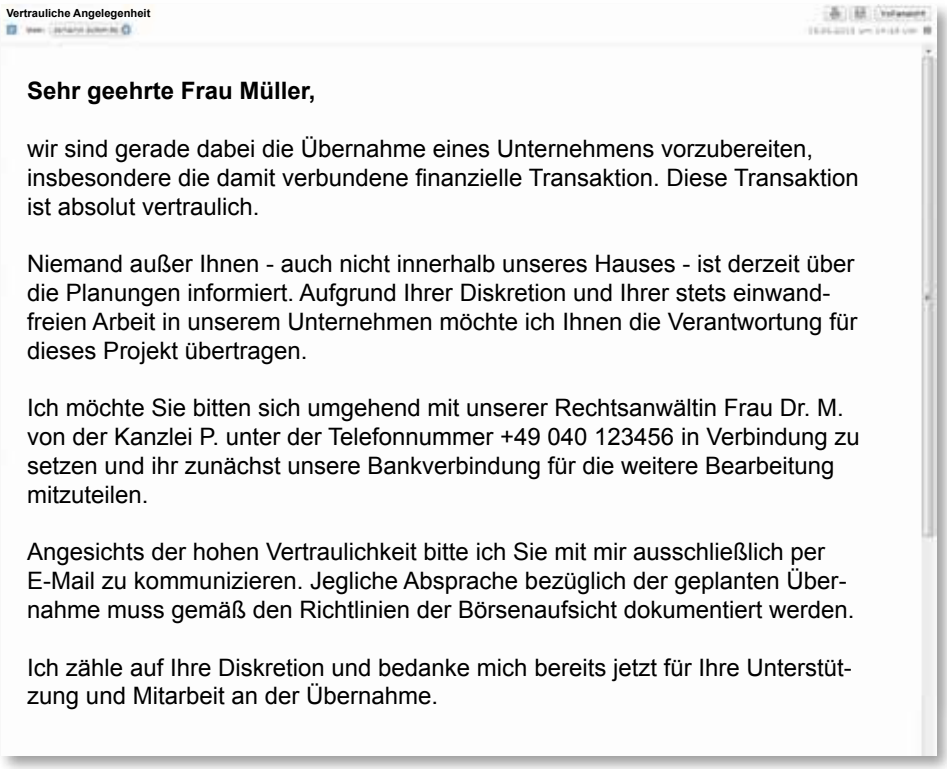
Weshalb ist so etwas überhaupt möglich?

Diese Angriffe zielen auf die Schwachstelle Mensch und nutzen fest eingeprägte Verhaltensmuster aus, beispielsweise Konsistenz. Konsistentes Verhalten bedeutet, in Übereinstimmung mit früherem Verhalten zu handeln. Die Gesellschaft bewertet konsistentes Verhalten als positive Charaktereigenschaft.

Angreifer gehen also davon aus, dass sich Mitarbeiter konsistent verhalten und die gefälschte E-Mail des Chefs als legitim einstufen. Um die Wahrscheinlichkeit noch zu erhöhen, spielen weitere Details eine entscheidende Rolle.

Statistisch gesehen ist der beste Zeitpunkt für die Zustellung der Betrugs-E-Mail Dienstag bis Donnerstag nach der Mittagspause. Der erste Klick erfolgt dabei innerhalb einer Stunde nach Eintreffen. Neben der Tageszeit können auch Jahreszeiten eine Rolle spielen, beispielsweise klassische Urlaubs- bzw. Vorurlaubszeiten. Im Fall von FACC erfolgte die erste Überweisung am 23. Dezember.

Bei professionellen Angriffen ist der Textinhalt der Betrugsmail genau auf die Firma und den Mitarbeiter abgestimmt. Ein reales Beispiel findet sich in einem Video auf der Schwerpunkt-Webseite „Cybercrime“ bei Euler Hermes.



Vertrauliche Angelegenheit

Sehr geehrte Frau Müller,

wir sind gerade dabei die Übernahme eines Unternehmens vorzubereiten, insbesondere die damit verbundene finanzielle Transaktion. Diese Transaktion ist absolut vertraulich.

Niemand außer Ihnen - auch nicht innerhalb unseres Hauses - ist derzeit über die Planungen informiert. Aufgrund Ihrer Diskretion und Ihrer stets einwandfreien Arbeit in unserem Unternehmen möchte ich Ihnen die Verantwortung für dieses Projekt übertragen.

Ich möchte Sie bitten sich umgehend mit unserer Rechtsanwältin Frau Dr. M. von der Kanzlei P. unter der Telefonnummer +49 040 123456 in Verbindung zu setzen und ihr zunächst unsere Bankverbindung für die weitere Bearbeitung mitzuteilen.

Angesichts der hohen Vertraulichkeit bitte ich Sie mit mir ausschließlich per E-Mail zu kommunizieren. Jegliche Absprache bezüglich der geplanten Übernahme muss gemäß den Richtlinien der Börsenaufsicht dokumentiert werden.

Ich zähle auf Ihre Diskretion und bedanke mich bereits jetzt für Ihre Unterstützung und Mitarbeit an der Übernahme.

Im Text finden sich einige wichtige Merkmale.

Wertschätzung

Das Opfer erfährt durch den Angreifer eine hohe Wertschätzung. Wer möchte nicht vom Chef für seine tadellose Arbeit gelobt werden?

Wissensalleinstellung

Mit der „Wissensalleinstellung“ bleiben keine weiteren Gesprächspartner im Unternehmen.

Monokommunikationsebene

In der Monokommunikationsebne E-Mail fehlen Absicherungsmechanismen (Stimme), die durch ein persönliches Gespräch transportiert werden.

Absolute Verschwiegenheit

Schließlich wird absolute Verschwiegenheit eingefordert. Diese „befohlene Mitarbeiterverschwiegenheit“ geht sehr weit: In einem Betrugsfall bei der Münchner Hofpfisterei überwies eine Mitarbeiterin der Buchhaltung 1,9 Millionen Euro nach Hongkong. Diese außergewöhnliche Überweisung löste keine Nachfrage aus, obwohl die Geschäftsführerin, deren E-Mailadresse gefälscht wurde, nur wenige Türen weiter saß. ▸

Der wichtigste Schutzschirm: die Mitarbeitersensibilisierung

In meinen Schulungen finden sich immer Teilnehmer, die von dieser Betrugsmasche noch nie gehört haben. Diese Kollegen wären klassische Opfer dieser Angriffsvariante.

Im Idealfall schaffen wir es also, allen Mitarbeitern die Betrugsmasche vorzustellen. Eine Möglichkeit wäre das genannte Video von Euler Hermes in die Datenschutz-Präsentation einzubauen. Ist die Masche bekannt, steigt die Wahrscheinlichkeit exponentiell, dass ein Betrugsversuch durch einen Mitarbeiter gemeldet wird.

Jeder Zeit einen Ansprechpartner

Mitarbeiter sollten motiviert werden ungewöhnliche Vorgänge jeder Art zu melden und Fehler einzugestehen. Für diesen Prozess muss ein Ansprechpartner mit Vertretung benannt werden. Die Ansprechpartner müssen kein tiefes Know-how im Thema haben. Hohes Vertrauen der Mitarbeiter und die pflichtbewusste Weitergabe der Anfrage an interne Spezialisten sind die wichtigsten Voraussetzungen.

Mitarbeitern müssen diese Ansprechpartner bekannt sein. Mindestens muss klar sein, in welchem Papierdokument die Kontaktdaten der Ansprechpartner hinterlegt sind. Die Papierform ist dabei wichtig, da diese auch eine Recherche zulässt, wenn kein Endgerät zur Verfügung steht.

Prüfen des Webseitenauftritts

Setzt sich das Unternehmen mit der Angriffsvariante CEO-Fraud auseinander, ist auch der Webseitenauftritt zu prüfen.

- Welche Interna geben die Webbeiträge preis?
- Welche Mitarbeiter sind aufgeführt?
- Welche Kontaktdaten werden angegeben?

Verwenden Sie praktische Beispiele

Wenn Mitarbeiter einen Betrugsfall melden, können Sie diese Muster sehr gut für Ihre Sensibilisierung nutzen. Erstellen Sie einen Screenshot und zeigen Sie in einer Rundmail, wie man diese Fälschung entlarven kann, beispielsweise

- falsche Domain
- unkorrekte Ansprache
- ungewöhnliche Vorgaben (absolute Verschwiegenheit)
- unvollständige Signatur.

Beziehen Sie die IT-Kollegen mit ein

Neben den organisatorischen Maßnahmen sollten technische Möglichkeiten eingesetzt werden. Hier gilt es den Administratoren den Ablauf des CEO-Fraud darzustellen, damit passende Lösungsansätze definiert werden können.

Diese müssen nicht immer hohe Geldbeträge bedeuten. Oft können einfache Maßnahmen das Risiko bereits deutlich reduzieren.

Steht der Firmenmailserver in der Firmendomain, kann es nicht sein, dass eine Nachricht mit @firma.de von außen an das Unternehmen zugestellt wird. Die Firewall kann alle eingehenden E-Mails, die die Firmendomain beinhalten, blocken und somit auch die Betrugsmail chef@firma.de an die Buchhaltung.

Fazit

Durch die oft individuelle Ansprache der Mitarbeiter sind zielsichere, technische Lösungen schwieriger zu implementieren. Wenn technische Lösungen versagen, fungieren sensibilisierte Mitarbeiter als „Human Firewall" und damit als wichtigster Schutzfaktor gegen diese Betrugsmasche.

Quellen: BKA, Christof Kerkmann, Lars-Marten Nagel, Euler Hermes, Bernhard Hecker

Über den Autor

Stefan Bachmann

ist seit 28 Jahren bei der INES IT im Südostbayerischen Unterneukirchen beschäftigt. Seit 2009 wirkt er am Aufbau der Abteilung Datenschutz- und IT-Sicherheit mit. Heute bietet die INES IT in diesem Bereich Datenschutz- und IT-Sicherheitsberatung, Schulungskonzepte, Securityaudits und Penetrationstests.

▶ www.ines-it.de

Anzeige

Seminare und Lehrgänge.

Für eine gesetzeskonforme und professionelle Umsetzung des Datenschutzes.

Seminare für die Praxis

Sichern Sie sich jetzt umfangreiches und aktuelles Know-how für Ihre persönliche berufliche Entwicklung.

TÜV Rheinland bietet ein breit gefächertes Portfolio an Bildungs- und Beratungsdienstleistungen auf höchstem fachlichen Niveau. Mehr als 7.500 Angebote, über 2.500 Referenten. Deutschlandweit.

Zum Thema Datenschutz bieten wir zahlreiche Seminare und modulare Lehrgänge mit der Möglichkeit, ein Zertifikat der unabhängigen Personenzertifizierungsstelle PersCert von TÜV Rheinland zu erwerben.

Datenschutz

Alle Seminare und Lehrgänge beziehen sich selbstverständlich auf die EU-DSGVO und das neue BDSG.

- Datenschutzfachkraft.
- Datenschutzbeauftragter (TÜV).
- Datenschutzauditor (TÜV).
- Externer Datenschutzbeauftragter (TÜV).
- EU-Datenschutz-Grundverordung.
- Datenschutzbeauftragter. Update auf die EU-DSGVO.
- EU-DSGVO und Informationssicherheit. Vom ISMS zum DSMS.
- Datenschutzwissen für Geschäftsführer.
- Umsetzung der neuen Datenschutzanforderungen für Kleinbetriebe.
- Das Standard-Datenschutz-Modell.
- Die DSGVO mit QM-Werkzeugen umsetzen
- Auftragsverarbeitung nach EU-DSGVO und neuem BDSG.
- Datenschutz Update – Fortbildung für Datenschützer.
- Übersicht der Verarbeitungstätigkeiten & Datenschutz-Folgenabschätzung.
- Videoüberwachung nach DSGVO und neuem BDSG.
- Grundlagen des Datenschutzes. Online-Training.
- Der rechtliche Rahmen des Datenschutzes. Online-Training.

Weitere Details, Seminare und Anmeldung unter:
www.tuv.com/datenschutz

Übrigens: Auch im Bereich Compliance finden Sie bei uns eine Vielzahl praxisorientierter Qualifizierungsangebote.

Weitere Details, Seminare und Anmeldung unter:
www.tuv.com/seminare-compliance

Weitere Informationen erhalten Sie auch bei:
TÜV Rheinland Akademie GmbH
Am Grauen Stein · 51105 Köln
Sandra Fahling · Tel. 0221 806-3561
sandra.fahling@de.tuv.com

www.akademie.tuv.com

TÜVRheinland®
Genau. Richtig.

DATENSCHUTZ ZUM ANFASSEN - WIE MIT EINEM „HACKERLABOR“ TECHNISCHE RISIKEN VERSTÄNDLICH VERMITTELT WERDEN

Thomas Floß

Eine der größten Herausforderungen der Datenschutz-Grundverordnung (DS-GVO) ist - neben den umfangreichen Transparenz- und Informationspflichten - der Bereich „Stand der Technik“. Die Artikel 25 und 32 DS-GVO, in denen dieser manifestiert ist, stellen sowohl Anwender als auch teilweise Datenschutzbeauftragte vor sehr große Herausforderungen. Nicht immer ist es einfach, ein angemessenes technisches Niveau zu vermitteln, sodass es der Datenschutz-Grundverordnung entspricht. Der Mensch muss mitgenommen werden, die Technik sowie deren Hintergrund verstehen und sich entsprechend verhalten.

Um dieser Herausforderung gerecht zu werden, hat die EDV-Unternehmensberatung Floß bereits vor vielen Jahren das sogenannte „Hackerlabor“ entwickelt. Das Hackerlabor soll Anwendern jeden Alters verständlich und bildlich untermauert vermitteln, wie Technik funktioniert und warum es zum Beispiel sinnvoll ist, Informationen zu verschlüsseln oder Webseiten sicher zu gestalten.

Das Hackerlabor wird in Form eines Vortrages mit direktem Teilnehmer-Dialog sowie Live-Hacking (legal und nach Zustimmung der Teilnehmer) durchgeführt und zeigt anschaulich Alltagsrisiken auf.

Inhaltlich geht es um die Themenschwerpunkte:

- Grundlagen Internet/Intranet,
- Manipulation und Spionage,
- Risiken mobiler Geräte,
- Unsichere Webseiten,
- Unachtsame Informationsverbreitung im Internet,
- Risiken von USB-Sticks.

Grundlagen Internet/Intranet – das World Wide Web (er)kennt Sie

Sie glauben nicht, dass Sie mit Ihren technischen Geräten weltweit eindeutig identifizierbar sind? Das geht auch vielen Schulungsteilnehmern so. Das Internet ist eine der wesentlichen Grundlagen unserer gesamten Kommunikationsstruktur. In gleicher Art und Weise wie das Internet funktioniert auch das interne „Intranet".

Um die Schulungsteilnehmer, die Mitarbeiter und die Verantwortlichen auf die digitale Reise mitzunehmen, ist es zunächst wichtig Grundlagen zu schaffen. Wie komme ich auf einen Webserver, was hinterlasse ich dabei an Informationen und warum sind diese Informationen in Bezug auf die Rückverfolgbarkeit so entscheidend bzw. so relevant?

Genau dieser Aspekt ist den meisten Nutzern nicht einmal ansatzweise präsent, obwohl jedes Smartphone, jeder Rechner und auch zunehmend Smartwatches eine weltweit eindeutige Kennung, die IP-Adresse, besitzen. Und mit dieser sind sie zu identifizieren.

Manipulation und Spionage – hier werden Sie gehackt

Im nächsten Schritt gilt es, die möglichen technischen Aspekte in Bezug auf Manipulation von Informationen, Spionage und Informationsbeschaffung zu vermitteln.

Hierzu gehört das Fälschen von IP-Adressen bzw. URL-Adressen (DNS-Spoofing), welches mit dem Hacking eines Standard-XING-Profils demonstriert wird.

Auch das Risiko eines zu simplen Passwortes wird mit Hilfe des Werkzeugs LophtCrack aufgezeigt und somit in einfacher Art und Weise leicht transparent gemacht.

Risiken mobiler Geräte – WhatsApp, iCloud, Google-Cloud

Eines der größten Risiken in der IT-Infrastruktur nutzt nahezu jeder Mitarbeiter mehrfach täglich: das Smartphone. Viele Mitarbeiter und häufig insbesondere das Management verkennen dabei die Bedeutung von Passwörtern und sonstigen Schutzmaßnahmen, weshalb dieser Aspekt von extremer Bedeutung ist. Gerade im Bereich des Managements wird sehr gerne WhatsApp auf den Smartphones installiert, private Fotos liegen selbstverständlich in der iCloud oder es erfolgt eine Vollsynchronisation mit der Google-Cloud.

Im Rahmen des Hackerlabors wird mit einem sehr wirkungsvollen Instrument, nämlich FlexiSPY, vorgeführt, was es bedeutet Daten in verschiedenster Art und Weise auf dem Smartphone ohne entsprechende Schutzmechanismen gespeichert zu haben, sodass ein möglicher Angreifer mittels trojanischem Pferd die gesamten Informationen abrufen kann. Im Vortrag greift die Unternehmensberatung Floß live auf WhatsApp-Daten zu.

Unsichere Webseiten – so wird bei Ihnen günstig eingekauft

Ein weiterer Schwerpunkt innerhalb des Hackerlabors ist die transparente Darstellung von „Privacy by Design" und die Notwendigkeit aktueller Webseiten.

In einer Live-Aufführung werden Shop-Daten manipuliert und Waren zu einem irrealen Preis in den Warenkorb gestellt. Einzig und allein das Abschicken erfolgt sodann nicht mehr live, da hier die Grenze in Richtung Strafgesetzbuch überschritten wäre.

Unachtsame Informationsverbreitung im Internet – hier kann es peinlich werden

Viele Menschen gehen unachtsam mit den Informationen um, die sie im Internet veröffentlichen.

Mit Hilfe des Werkzeugs Maltego lassen sich diese Menschen und deren Informationen mit einer sehr hohen prozentualen Quote grafisch darstellen. Dies erschüttert die Teilnehmer sehr häufig, da sie niemals vermutet hätten, dass man so einfach an Informationen – manchmal auch sehr peinliche Informationen – gelangen kann.

Anschließend wird darauf eingegangen, was Bildinformationen verraten. Denn kaum ein Teilnehmer hat jemals von Metadaten und GPS-Informationen in Fotodaten gehört. So ist es zum Beispiel ohne großen Aufwand möglich, zahlungskräftige Kunden herauszufinden. Ein simples Beispiel: Ein Handwerker fotografiert sein Unikat in Form eines besonderen Wohnzimmerschranks mit dem Smartphone bei eingeschalteter GPS-Kennung und stellt das Bild 1:1 direkt auf seiner Webseite. Hier findet sich zunächst kein ▸

Personenbezug, jedoch lässt sich durch die GPS-Kennung der Standort des Wohnzimmerschranks herausfinden. Und mithilfe weiterer Recherche zu dem Standort kann so eine extrem relevante und sensible Information ermittelt werden.

Risiken von USB-Sticks – gelöscht ist nicht gleich gelöscht

In einem Live-Experiment wird abschließend verdeutlicht, wie gefährlich das Einstecken eines USB-Sticks im eigenen System ist und welche vollautomatischen Abläufe stattfinden. Viele Teilnehmer können sich sicher auch nicht vorstellen, dass man Daten auf formatierten Speicherkarten ihres Fotoapparates oder Camcorders ohne Weiteres wiederherstellen kann. Um dieses greifbar darzustellen, wird dieser Vorgang live durchgeführt, sofern uns die Teilnehmer Speicherkarten mit ihren eigenen Informationen zur Verfügung stellen.

Das Hackerlabor wird inzwischen seit fast zehn Jahren durchgeführt, fortlaufend erweitert und verbessert. Nach dem Ende des Dialogvortrages sind die Teilnehmer nachhaltig sensibilisiert und verändern - zumindest in Teilen - ihr Nutzungsverhalten. Ein solches Hackerlabor kann und darf allerdings keine einmalige Aktion sein, denn gerade in Bezug auf die Sensibilisierung ist Nachhaltigkeit gefordert. Das Hackerlabor ist grundlegend nur der Auftakt für weitere ergänzende oder parallel stattfindende Aktionen. Beispielsweise Security-Awareness-Kampagnen in Form von gefälschten E-Mails, simulierten Anrufen bzw. in Form von gefälschten Downloadfiles, die sogenannte trojanische Pferde beinhalten.

Eine nachhaltige und sinnvolle Sensibilisierung von den technischen Aspekten, die im Artikel 25 und 32 festgelegt sind, kann mit einer entsprechenden Untermauerung durch solche Kampagnen erfolgen.

Über den Autor

Thomas Floß

Geschäftsführer,
EDV-Unternehmensberatung Floß GmbH
Datenschutz- und Informationssicherheitsberater

▶ www.floss-consult.de

EDV-Unternehmensberatung
Floß GmbH

Anzeige

RHENUS LOGISTICS

RHENUS DATA OFFICE GMBH

IHR KOMPETENTER PARTNER FÜR DIE AKTEN- UND DATENTRÄGERVERNICHTUNG

Vertrauen Sie auf das Leistungspotential und Know-how eines seit vielen Jahren führenden Dienstleisters in der Dokumentenlogistik

- MOBILE UND STATIONÄRE AKTEN- UND DATENTRÄGERVERNICHTUNG
- OFFICE-ENTSORGUNGEN
- 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

DIE EPRIVACY-VERORDNUNG – EINE VERORDNUNG FÜR EINE DATENSCHUTZGERECHTE ELEKTRONISCHE KOMMUNIKATION?

Prof. Dr. Anne Riechert

Am 23.10.2018 veranstalteten die Stiftung Datenschutz und die DIHK gemeinsam eine Tagung zum Thema „E-Privacy-Verordnung, Was kommt auf uns zu?"[1]

Nach den zahlreichen Debatten über die Datenschutzgrundverordnung beschäftigt nun die Frage nach einem Datenschutz für elektronische Kommunikationsvorgänge Unternehmen und Datenschutzaktivisten gleichermaßen. In der Vergangenheit stellte es bislang stets eine Herausforderung dar, Datenschutzrecht leicht verständlich zu vermitteln. In dieser Tradition stellt auch die ePrivacy-Verordnung keine einfache Lektüre dar. Was bedeutet diese für Bürger? Welche Konsequenzen ergeben sich für Unternehmen? Insbesondere die Betroffenenrechte wurden durch das Publikum der Fachtagung konkret und kritisch angesprochen. Die Fragen bezogen sich u.a. auf die Möglichkeiten für Unternehmen, Daten der elektronisch geführten Kommunikation auswerten zu können. Im Mittelpunkt steht der Begriff der so genannten Kommunikationsmetadaten (beispielsweise angerufene Nummern, besuchte Websites, der geografische Standort, Uhrzeit, Datum und Dauer eines von einer Person getätigten Anrufs). Erwägungsgrund 2 des Entwurfs der ePrivacy-Verordnung führt dazu aus, dass sich aus diesen Daten präzise Schlussfolgerungen über das Privatleben der an der elektronischen Kommunikation beteiligten Personen ziehen lassen, z. B. in Bezug auf ihre sozialen Beziehungen, Gewohnheiten und ihren Lebensalltag, ihre Interessen, ihren Geschmack. Die besondere Schutzwürdigkeit von Kommunikationsmetadaten wurde zudem durch den Europäischen Gerichtshof betont. Trotz dieser konstatierten Sensibilität der Metadaten geht die geplante ePrivacy-Verordnung nun über das hinaus, was bislang galt. Dies wird insbesondere von Verbraucherschützern mit dem Hinweis kritisiert, dass die Verarbeitung von solchen Metadaten nach dem Telekommunikationsgesetz weitaus eingeschränkter zulässig war und auch die ▸

[1] Weitere Informationen zur Veranstaltung und zum Inhalt der ePrivacy-Verordnung sind unter stiftungdatenschutz.org abrufbar. Dort ist auch der Hinweis zu finden, dass derzeit nicht absehbar ist, wann Trilog-Verhandlungen stattfinden.

Verarbeitung von Inhaltsdaten sei bisher nicht erlaubt gewesen.[2]

Vieles ist noch im Fluss, aber der Vorschlag unter der österreichischen Ratspräsidentschaft bringt die Datenverarbeitung für „kompatible" Zwecke ins Spiel (Artikel 6 Absatz 2a).[3] Eine solche Möglichkeit war im Entwurf der Europäischen Kommission vom 10.01.2017[4] und der bulgarischen Präsidentschaft vom 04.05.2018[5] noch nicht enthalten und könnte eine umfassende Verarbeitung von diesen sensiblen Kommunikationsmetadaten zur Folgen haben – je nachdem wie weit „kompatible Zwecke" in der Praxis ausgelegt werden. Der Nutzen für Big Data liegt dabei auf der Hand. Allerdings wurde die rechtliche Grundlage für Big-Data-Anwendungen bereits ohne diese inhaltliche Erweiterung gelegt. So ermöglicht auch der Entwurf der bulgarischen Ratspräsidentschaft die Verarbeitung von pseudonymisierten Geodaten (Artikel 6 Absatz 2e) und die Verarbeitung für statistische Zwecke oder wissenschaftliche Forschungszwecke, sofern dies durch die DS-GVO oder durch das Recht der einzelnen Mitgliedstaaten geregelt ist (Artikel 6 Absatz 2f).[5] Die Möglichkeit der Verarbeitung von pseudonymisierten Kommunikationsmetadaten im Rahmen von Big Data und auf der Grundlage der ePrivacy-Verordnung wurde auch von Dr. Daniela Brönstrup, BMWi, genannt, die im Rahmen der Veranstaltung insgesamt über den Verhandlungsstand in Brüssel informierte.

Grundsätzlich werden in Big-Data-Anwendungen große Chancen gesehen. Es drängt sich also die Frage auf, aus welchem Grunde der Entwurf von vielen Unternehmen kritisiert wird. Die Antwort darauf sind insbesondere die Interessen der kleinen und mittelständischen Unternehmen, die eine Vielzahl von Verpflichtungen befürchten ohne von den Möglichkeiten einer großflächigen Big-Data-Anwendung profitieren zu können. Ihre Geschäftsmodelle konzentrieren sich regelmäßig nicht auf umfassende Datenauswertungen. Zudem sind einige Unternehmen mangels ausreichender Kapazitäten derzeit weiterhin damit beschäftigt die Vorgaben der Datenschutzgrundverordnung konform umzusetzen. Ein weiteres umfassendes Regelwerk würde aus ihrer Sicht eine erneute Belastung darstellen, worauf ebenso Herr Klemens Gutmann, regiocom, nochmals eindringlich hinwies. In diesem Zusammenhang ist ergänzend das Bayerische Landesamt für Datenschutzaufsicht positiv hervorzuheben. Diese Aufsichtsbehörde hat bereits frühzeitig Hilfestellungen für kleine und mittelständische Unternehmen zur Umsetzung der Datenschutz-Grundverordnung veröffentlicht, die an praxisgerechten Beispielen aufzeigen, wie etwa ein Verzeichnis von Verarbeitungstätigkeiten auszufüllen ist und welche Anforderungen die Unternehmen nochmals genauer prüfen sollten.[6] Ist daher die Erstellung solcher Praxishilfen zukünftig ebenso im Rahmen der Umsetzung der ePrivacy-Verordnung notwendig? Einerseits muss die Erforderlichkeit der Bereitstellung praxisgerechter Orientierungshilfen durch die Aufsichtsbehörden klar bejaht werden, wobei Frau Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen, in ihrem Vortrag gleichermaßen die Verantwortung der Politik betonte. Andererseits ist an dieser Stelle auf die notwendige Harmonisierung der Verordnung in den europäischen Mitgliedstaaten hinzuweisen. Der Entwurf konzentriert sich ausweislich seines Erwägungsgrundes 39 darauf, dass *„die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten werden, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen zu berücksichtigen."* Um jedoch von vorneherein eine europaweite Harmonisierung herzustellen, könnten klar formulierte Anwendungsregelungen für diese Unternehmen unmittelbar im Verordnungstext verankert werden. Dies wäre ein Wunsch der genannten Kleinstunternehmen, aber die Politik muss dies entsprechend mittragen.

Darüber hinaus müssen aber wie eingangs erwähnt ebenso die Rechte der Bürger besonders beleuchtet werden. Können die Bürger überhaupt absehen, was auf sie zukommt? Eine der Hauptaufgaben wird sein, den betroffenen Personen die Datenverarbeitung in leicht verständlicher Form zu erklären. Umfassende und unbestimmte Regelungen, wie die Verarbeitungsmöglichkeit zu den bereits oben genannten kompatiblen Zwecken, stehen diesem Transparenzgedanken entgegen. Aber auch der Entwurf der Europäischen Kommission und die Änderungsvorschlage des EU-Parlaments sowie der bulgarischen Ratspräsidentschaft beinhalten

[2] Siehe https://www.vzbv.de/sites/default/files/downloads/2018/09/26/18-09-24_vzbv-kernpositionen_eprivacy-vo.pdf.

[3] ePrivacy-VO-Rat, Ratsdokument 13256/18 vom 19.10.2018, abrufbar unter https://www.parlament.gv.at/PAKT/EU/XXVI/EU/03/91/EU_39172/imfname_10848802.pdf.

Entwurf der Europäischen Kommission vom 10.01.2017 (COM(2017) final 2017/0003 (COD), abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52017PC0010.

[4] Siehe den Entwurf zur ePrivacy-Verordnung der bulgarischen Präsidentschaft vom 04.05.2018, abrufbar unter http://data.consilium.europa.eu/doc/document/ST-8537-2018-INIT/en/pdf.

[5] Siehe den Entwurf zur ePrivacy-Verordnung der bulgarischen Präsidentschaft vom 04.05.2018.

[6] Siehe die Handreichungen für KMUs, abrufbar unter https://www.lda.bayern.de/de/kleine-unternehmen.html.

bereits umfangreiche und nicht leicht zu durchdringende Regelungen zur Verarbeitung von Kommunikationsdaten oder zur Erhebung und Nutzung von Informationen. Ist ein Bürger tatsächlich in der Lage zu verstehen, zu welchem Zweck und für welchen Zeitraum die Verarbeitung seiner schützenswerten Daten stattfinden darf? Dies wird zukünftig eine immense Herausforderung darstellen.

Weiterhin ist darauf zu verweisen, dass der aktuelle Entwurf des Rates die vollständige Streichung von Artikel 10 vorsieht. Ursprünglich waren in dieser Regelung Browserlösungen vorgesehen, die ein Einverständnis der Nutzer in Trackingmaßnahmen, wie etwa Cookies, vorsehen. Die Software musste den Endnutzer über die Einstellungsmöglichkeiten zur Privatsphäre informieren und zur Fortsetzung der Installation vom Endnutzer die Einwilligung zu einer Einstellung verlangen. Die Einwilligungslösung entspricht im Übrigen der Position der Datenschutzkonferenz.[7] Danach bedarf es jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und ebenso bei der Erstellung von Nutzerprofilen. An dieser Auffassung wurde vehement Kritik geäußert und es wird sich zeigen, ob die Aufsichtsbehörden sie zukünftig beibehalten werden. Geändert wurde Artikel 10 im Übrigen bereits durch den Entwurf des Rates vom 04.05.2018, der anstatt einer Einwilligung lediglich eine Information über die Privatsphäreeinstellungen vorsieht. Eine vollständige Streichung dieser Regelung würde nun dazu führen, dass gleichermaßen Artikel 23 geändert werden muss und keine Sanktionen mehr für Hersteller vorgesehen sind, die der Verpflichtung nach Artikel 10 nicht nachkommen. In diesem Zusammenhang muss ebenso erwähnt werden, dass außerdem eine Regelung für erforderlich gehalten wird, die sicherstellt, dass eine Einwilligung in Cookies für werbefinanzierte Inhalte verlangt werden kann. Auf eine solche Möglichkeit wies Herr Rolf Bender, BMWi, im Rahmen der ePrivacy-Veranstaltung hin. Dieses Vorhaben wurde mit dem Argument kritisiert, dass gerade ausgeschlossen sein soll eine für die Vertragserfüllung nicht notwendige Datenverarbeitung zum Vertragsgegenstand zu machen.[8]

Es ist in der Praxis umstritten, inwieweit die gerade genannten Browserlösungen tatsächlich ein zweckdienliches Mittel darstellen. Dennoch verschaffen sie einem Nutzer zunächst die notwendige Kontrolle über seine Daten. Kann sich eine solche Lösung nicht durchsetzen und werden aber dennoch weiterhin Geschäftsmodelle mit den Nutzerdaten betrieben, muss in irgendeiner Form die notwendige Transparenz für die betroffene Person hergestellt werden. Sie muss zumindest in der Lage sein zu verstehen und zu entscheiden, welche Kommunikationsdaten verarbeitet werden. Ansonsten bleibt der „Selbstdatenschutz". Entsprechende Technik, die Nutzerverhalten im Rahmen von Trackingmaßnahmen verschleiert, gibt es bereits auf dem Markt. Die Frage ist nur, inwiefern Nutzer ebenso bereit sind, Geld für Datenschutz auszugeben. Dies kann auch die ePrivacy-Verordnung nicht regeln.

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

[7] Papier zur Positionsbestimmung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder zur Anwendbarkeit des TMG für nicht-öffentliche Stellen vom 26. April 2018 – abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2018/2018-DSK-Positionsbestimmung_TMG.pdf.

[8] Siehe auch WP 259 der Artikel-29-Datenschutzgruppe vom 10.04.2018, abrufbar unter https://www.datenschutzkonferenz-online.de/media/wp/20180410_wp259_rev01.pdf. Ansinnen des Europäischen Parlaments war es außerdem, dass die ePrivacy-Verordnung die Verwendung von sogenannten Cookie-Mauern und Cookie-Bannern verhindern sollte (siehe Erwägungsgrund 22 im Vorschlag des EU-Parlaments – Entwurf einer legislativen Entschließung des Europäischen Parlaments vom 23.10.2017. Eine Synopse ist abrufbar unter https://www.lda.bayern.de/media/eprivacy_synopse.pdf).

DIE BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT IM GESPRÄCH MIT DER BVD-NEWS REDAKTION

Andrea Voßhoff im Interview

Andrea Voßhoff

Frau Voßhoff, mit dem Start der DS-GVO trat der Datenschutz in Europa in eine neue Epoche ein - aber noch viele Fragen sind offen. Was sind Ihrer Einschätzung nach die dringendsten Aufgaben (für Politik, DSB, BfDI) für die nächsten Monate?

In den letzten Wochen waren verschiedene 100-Tage-Bilanzen zur DS-GVO zu lesen und es hat sich gezeigt, dass viele der um den 25. Mai 2018 in der Öffentlichkeit kursierenden Befürchtungen, wie beispielsweise das Ende der Fotografie oder eine große Abmahnwelle, ausgeblieben sind. Das ist erstmal erfreulich. Gleichwohl wird aber auch deutlich, dass der Informationsbedarf insbesondere für Bürger, Vereine und Verbände nach wie vor sehr hoch ist. Hier sollte auch die Politik einen Handlungsauftrag für entsprechende Informationskampagnen erkennen. Rufe nach Änderungen der DS-GVO sind vorschnell, denn die Auswirkungen einer so großen Reform lassen sich nicht bereits nach wenigen Monaten abschätzen. Die DSB haben aus meiner Sicht in erster Linie die Aufgabe, den Implementierungsprozess in den Unternehmen und Behörden zu begleiten und zu kontrollieren. Für die BfDI und die Aufsichtsbehörden der Länder gehört zu den drängendsten Aufgaben in erster Linie die Bewältigung der mit der DS-GVO einhergehenden großen personellen und organisatorischen Herausforderungen. Durch die DS-GVO hat sich das Bewusstsein für Datenschutzfragen und damit der Beratungsbedarf stark erhöht und die Anzahl an Eingaben und Beschwerden ist signifikant gestiegen.

Viele Unternehmen hatten zum Start der DS-GVO nur rudimentäre Anforderungen umgesetzt. Wie lassen sich diese zu weiterem Engagement für mehr Datenschutz motivieren?

Inzwischen sind viele Unternehmen bei der Umsetzung der DS-GVO nach meinem Kenntnisstand gut vorangekommen. Der Stellenwert des Datenschutzes wird mit zunehmender Digitalisierung auch zum Gradmesser des Vertrauens für Kunden in ein Unternehmen. Den Datenschutz daher nicht als bürokratisches Hemmnis, sondern vielmehr als Qualitätsmerkmal zu verstehen, kann im Wettbewerb um Kundinnen und Kunden daher entscheidende Motivation für Unternehmen sein, dauerhaft erfolgreich am Markt zu bestehen.

Wie wichtig und sinnvoll halten Sie strenge Kontrollen?

Die Kontrolle ist ein zentraler Aspekt bei der Durchsetzung des Datenschutzrechts. Bei der BfDI gilt seit jeher das Motto, mit der Kontrolle auch Beratung und Information zu verbinden, um den Institutionen zu helfen, das zum Teil komplexe Recht auch in der täglichen Arbeit umzusetzen. Angesichts der begrenzten Personalausstattung der Datenschutzaufsichtsbehörden in ganz Europa ist aber auch klar, dass die Einhaltung der DS-GVO nicht allein dadurch gewährleistet werden kann, dass alle datenverarbeitenden Stellen flächendeckend und umfassend kontrolliert werden. Mindestens ebenso wichtig ist das für Betroffene in Art. 77 DS-GVO verbriefte Recht auf Beschwerde bei einer Aufsichtsbehörde. Zum einen erhält hierdurch der Betroffene einen zusätzlichen außergerichtlichen Rechtsbehelf, zum anderen erhalten die Aufsichtsbehörden Hinweise auf konkrete Datenschutzverstöße.

Wie sehen Sie die Rolle der behördlichen Datenschutzbeauftragten/des Datenschutzbeauftragten bei Behörden und Einrichtungen des Bundes?

Die behördlichen Datenschutzbeauftragten haben eine zentrale Rolle bei der Selbstkontrolle sowie bei der Beratung der jeweiligen Behörde in Datenschutzfragen. Es obliegt ihnen auch, zu überwachen, ob ihre Dienststelle die Vorgaben der einschlägigen Datenschutzregelungen einhalten. Sie sind daher für die Aufsichtsbehörden eine wichtige Anlaufstelle.

Welche Handhabe hat Ihre Behörde?

In Art. 58 DS-GVO sind verschiedene Untersuchungs- und Abhilfebefugnisse der Aufsichtsbehörden geregelt. Diese reichen von der Verpflichtung des Verantwortlichen, Informationen zur Verfügung zu stellen über eine Warnung des Verantwortlichen bis hin zu einer Weisung, eine rechtswidrige Datenverarbeitung zu unterlassen und der Verhängung von Geldbußen.

Welche Befugnisse hätten Sie sich für mehr Durchsetzungskraft während Ihrer Amtszeit gewünscht?

Der Großteil meiner Aufsichtszuständigkeit betrifft öffentliche Stellen. Hier können Durchsetzungsprobleme bei der Ausübung bzw. Vollstreckung von Abhilfebefugnissen bestehen. So dürfen beispielsweise gegenüber öffentlichen Stellen keine Geldbußen verhängt werden. Außerdem kann ich gegenüber Behörden weder die sofortige Vollziehung von Maßnahmen anordnen noch meine Anordnungen vollstrecken, was zu einem Durchsetzungsdefizit führen könnte. Insbesondere im Bereich Polizei und Justiz, also außerhalb des Anwendungsbereichs der DGSVO, hätte ich mir wirksame Kontroll- und Durchsetzungsbefugnisse gewünscht. Mein Haus hat hier bislang – außer einer Anordnungsbefugnis gegenüber dem BKA nach Beanstandung erheblicher Verstöße – keinerlei echte Durchsetzungsbefugnisse.

Bei festgestellten Verstößen besteht nur die Möglichkeit einer Beanstandung. Dies halte ich für einen Verstoß gegen die Vorgaben der EU-Richtlinie für den Datenschutz bei Polizei und Justiz.

Sie galten bei Ihrem Antritt als Datenschutz-skeptisch. Was hat sich für Sie durch die Aufgabe der Bundesdatenschutzbeauftragten verändert?

Bei meiner Tätigkeit als Bundesdatenschutzbeauftragte war es mir von Anfang an wichtig, das Grundrecht auf informationelle Selbstbestimmung in den Mittelpunkt zu stellen, also den Schutz des Menschen und nicht den Schutz der Daten. Daran hat sich nichts geändert.

Bei Ihrer ersten Rede nach Amtsantritt auf dem Verbandstag des BvD nannten Sie die Mitglieder des BvD „Ihre Kollegen". Der DSB ist ein wichtiger gesetzlicher Baustein bei der Umsetzung des Datenschutzrechts für die Unternehmen. Was wünschen Sie sich für „Ihre Kollegen"?

Meinen Kolleginnen und Kollegen wünsche ich stets Freude, Beharrlichkeit und Fortune bei ihrer täglichen Arbeit, die mit dem 25. Mai 2018 nicht einfacher geworden ist. Vor allem aber wünsche ich ihnen eine Haus- und Unternehmensleitung, die erkennt, dass die Arbeit des DSB ein entscheidender Baustein für die Qualität behördlichen Handelns und für den unternehmerischen Erfolg ist.

Welche Bereiche des Datenschutzes sollten aus Ihrer Sicht in Zukunft eine besondere Rolle spielen?

Für uns alle sollten Fragen des Datenschutzes für Kinder von besonderer Bedeutung sein. In Bildungsinitiativen und Lehrplänen zur Stärkung der Medienkompetenz von Kindern und Jugendlichen muss die Vermittlung des Datenschutzes von Anfang an mitgedacht werden.

Mit der Initiative „Datenschutz geht zur Schule" hat der BvD hierzu eine wichtige Initiative gestartet. Diese Initiative sollte von der Politik aufgegriffen und verstetigt werden.

Vielen Dank für das Interview, Frau Voßhoff.

BvD-News: Katrin Eggert

WIE MACHT MAN DEN DATENSCHUTZ UNTER DER DS-GVO BESSER?

Dr. Stefan Brink

Dr. Stefan Brink

Im Moment beobachten wir eine Art „Gegen-Reformation" gegen die Datenschutz-Grundverordnung. Nach dem Datenschutz-Hype, den wir rund um den Mai 2018 miterleben durften, kommt jetzt die Gegenbewegung zu Wort, die den Datenschutz schon immer für überflüssig bis gefährlich hielt. Mit Meldungen wie der zum angeblich von der DS-GVO aufoktroyierten Abmontieren hunderter Klingelschilder in Wien wird eine Geschichte von einem kleinkarierten, beschränkenden, beschränkten und völlig widersinnigen Datenschutz erzählt, der mit seinen vollständig bürokratischen Regeln Unternehmen gängelt und Rechtsunsicherheit verbreitet.

Dabei geraten die wirklichen Errungenschaften der Datenschutz-Grundverordnung für die Betroffenenrechte aller Bürgerinnen und Bürger in Vergessenheit, und auch der Umstand, dass viele dieser Regelungen gar nicht so neu sind, sondern schon seit Jahren Bestand haben – und von den Datenschützern größtenteils mit Augenmaß und Praxisbezug umgesetzt worden sind.

Auch angesichts der Widerstände, die sich aktuell gegen die ePrivacy-Verordnung regen, ist mit der Datenschutz-Grundverordnung ein großer Wurf gelungen. Jetzt gilt es, ihren Regeln in der Praxis effektive Geltung zu verschaffen. Dabei stehen nicht nur die Verantwortlichen in der Pflicht, sondern auch die Aufsichtsbehörden und die Datenschutzbeauftragten. Letztere stehen in den Unternehmen und Behörden an vorderster Front – oft kämpfen sie darum, dass dem Thema Datenschutz überhaupt die richtige Aufmerksamkeit geschenkt wird und dass Verantwortung für dieses ebenso wichtige wie aktuelle Thema nicht bei ihnen abgeladen, sondern auch von der Geschäftsleitungsebene wahrgenommen wird. Den Datenschutz grundlegend in den Prozessen und Abläufen des jeweiligen Unternehmens zu verankern und nicht nur als Feigenblatt vor sich her zu tragen, ist eine wirklich große Aufgabe der betrieblichen wie auch der behördlichen Datenschutzbeauftragten.

Nach 150 Tagen DS-GVO haben die Aufsichtsbehörden eine Menge Erfahrung gesammelt – nicht nur dazu, an welchen Stellen Unternehmen der „datenschutzrechtliche Schuh" drückt, sondern auch, wie einige Betriebe die Herausforderungen der DS-GVO besonders gut gemeistert haben. Das gibt uns eine gute Grundlage für unsere Beratungen: Welche Themen der DS-GVO sollten vorrangig angegangen werden, welche kommen erst in 2. Linie in den Fokus und gibt es sogar Probleme, die getrost zurückgestellt werden können? In welchen Bereichen lohnt es sich, besonders vertieft anzusetzen und in welchen geht es eher darum, sich Schritt für Schritt hineinzuarbeiten? Und natürlich sollten die Aufsichtsbehörden die Frage beantworten, wo durch sie selbst künftig verstärkt geprüft und wo eher noch gewartet wird.

Dazu gibt dieser Beitrag die folgenden 10 Tipps, und zwar unterteilt in die Aufgabengebiete „Arbeit im betreuten Unternehmen" (Inhouse), „Verbesserung des eigenen Arbeitsablaufs" (Work

in Progress) und „Kontakte nach Außen“ (Foreign Affairs):

I. Inhouse

Tipp 1: Zuerst einmal ist interne **Überzeugungsarbeit** zu leisten. Die **DS-GVO bietet gerade den Unternehmen viele Vorteile**, die für die Entscheidungsträger nicht immer auf Anhieb ersichtlich und greifbar sind. Aufgrund ihres einheitlichen Ansatzes schafft die DS-GVO einen verbindlichen Rechtsrahmen für alle Unternehmen in der EU, die ihren Sitz in der EU haben oder hier ihren Geschäften nachgehen. Dabei erweist sich das Marktortprinzip des Art. 3 DS-GVO als nachhaltiger Garant für eine gleichmäßige Anwendbarkeit der Verordnung und damit gleiche rechtliche Verpflichtungen und Bedingungen innerhalb der Europäischen Union. Dieser offensichtliche Vorteil der DS-GVO, dass künftig innerhalb der EU gleiches Recht gleichmäßig zur Anwendung kommt und damit gleicher unternehmerischer Aufwand zu betreiben ist, wird durch das Marktortprinzip auf die globale Ebene ausgeweitet: Auch jedes außereuropäische Unternehmen, das in Europa seinen Markt sucht, das seine Dienstleistungen hier anbietet und hier seine Kunden hat, unterliegt der DS-GVO. Guter Datenschutz im deutschen Unternehmen wird dadurch nicht länger zum Wettbewerbsnachteil gegenüber jenen Konkurrenten, die sich bislang nicht um die Rechtsvorgaben des Datenschutzes gekümmert haben und sich die notwendigen Aufwände meinten sparen zu können – alle trifft die gleiche Rechtspflicht, die von den Aufsichtsbehörden (auch durch exorbitante Bußgelder) durchgesetzt werden wird.

Ein weiterer Vorteil: Nach dem so genannten One-Stop-Shop-Prinzip des Art. 56 DS-GVO ist bei grenzüberschreitenden Verarbeitungen nur noch eine, nämlich die federführende Aufsichtsbehörde am Sitz der „Hauptniederlassung” zuständig. Eine langwierige Abstimmung mit den Aufsichtsbehörden anderer Mitgliedstaaten ist für Unternehmen damit nicht mehr notwendig. Das spart Zeit und Kosten.

Insgesamt gilt also: Gerade die verschärften Möglichkeiten zu Sanktionen sorgen für mehr Wettbewerbsgleichheit: Unternehmen, die sich bisher nicht an die Datenschutzgesetze gehalten haben, müssen nun mit ernsthaften Konsequenzen rechnen, die ihren „Vorteil“, nicht in den Datenschutz investiert zu haben, aufheben.

Tipp 2: Ein betrieblicher Datenschutzbeauftragter ist für das Unternehmen von unschätzbarem Wert – und diesen Wert sollte der Datenschutzbeauftragte seiner Unternehmensleitung vor Augen führen. Im Idealfall agiert er als eine Art **Frühwarnsystem** und damit als **Schutzschild der Geschäfsführung**. Denn er kann diese frühzeitig auf Fehlentwicklungen und Pflichtverletzungen im Unternehmen hinweisen und damit deren Haftung nach § 130 OWiG verhindern: Es wird immer noch zu wenig darüber diskutiert, dass jeder Datenschutzverstoß im Unternehmen von den Aufsichtsbehörden daraufhin untersucht wird, ob die Leitungsebene diesen Verstoß durch mangelnde Schulung und Aufsicht in Sachen Datenschutz mit zu verantworten hat. dann liegt nämlich eine Aufsichtspflichtverletzung nach § 130 OWiG vor, die mit massiven Bußgeldern geahndet werden kann. Und gerade hier entlastet ein gut ausgebildeter, gut fortgebildeter und gut ausgestatteter Datenschutzbeauftragter die eigene Unternehmensleitung eminent. Darüber sollte er mehr reden!

Tipp 3: Um seiner Arbeit auch sachgerecht nachgehen zu können, muss der Datenschutzbeauftragte selbst ausreichend qualifiziert und mit den nötigen Ressourcen ausgestattet sein. Daneben hat es sich aber als sinnvoll erwiesen, **Schulungen auch für die Mitarbeiter** anzubieten und diese so für die im jeweiligen Unternehmen besonders relevanten Themen zu sensibilisieren und Berührungsängste zum Thema Datenschutz abzubauen. So wird ein Klima geschaffen, in dem eine vertrauensvolle Zusammenarbeit von Datenschutzbeauftragtem und (sonstigen) Mitarbeitern möglich ist – und wesentlich seltener Datenschutzverstöße passieren. Solche Schulungen kann man auch niedrigschwellig anbieten, etwa indem man auf einer Personalversammlung in 20 Minuten erklärt, welche Risiken bei der Nutzung von Social Media bestehen oder warum eine technisch saubere Löschung von Daten nicht nur personenbezogene Informationen schützt, sondern auch Betriebs- und Geschäftsgeheimnisse.

Tipp 4: Schließlich sollte der Datenschutzbeauftragte seine **eigene Tätigkeit im Unternehmen sichtbar machen**. Dies kann durch die feste Teilnahme an Meetings und Berichte von diesen in Mitarbeiterversammlungen über eine eigene Rubrik im Intranet bis hin zur Erstellung eines jährlichen Tätigkeitsberichts reichen. Auch hier kommt es nicht darauf an, erschöpfende Darstellungen zu verfassen, sondern durch präzise Hinweise auf gelöste Fragestellungen, auf begleitete Prozesse oder erzielte Fortschritte den Wert der eigenen Arbeit im Unternehmen zu verdeutlichen.

II. Work in Progress

Tipp 5: Mit der DS-GVO kommen eine Reihe an **Dokumentations- und Rechenschaftspflichten** auf die Verantwortlichen zu. Diesen ohne ein professionelles Datenmanagement-System nachzukommen oder aber ein solches aufzubauen kann gerade am Anfang „überwältigend“ sein. Hier sollte man nach der **„Methode Eichhörnchen“**, d. h. Schritt für Schritt, vorgehen und sich diejenigen ▸

Pflichten heraussuchen, die am wichtigsten für das eigene Unternehmen sind – und sich aktuell auch tatsächlich umsetzen lassen. Getreu dem Motto: Die DS-GVO bringt so viele unterschiedliche Aufgaben für den Datenschutzbeauftragten mit, da sollte er mit denjenigen beginnen, bei denen sich relativ rasch ein sichtbarer Fortschritt erzielen lässt.

Das kann neben dem Mitwirken bei der Erstellung des Verarbeitungsverzeichnisses etwa die Verpflichtung der Mitarbeiter auf das Datengeheimnis sein, ein Muster für Auftragsdatenverarbeitungen oder ein Ablaufplan für Auskunftserteilungen oder für den Umgang mit Datenpannen. Auch die Bestellung oder Fortbildung des Datenschutzbeauftragten sollte ebenso dokumentiert werden wie das Anfertigen einer Datenschutz-Folgenabschätzung – auch wenn sie nicht zum Ergebnis gelangt, dass die Aufsichtsbehörde einzuschalten ist. Jeder neue Prozess bringt das Unternehmen einen Schritt nach vorne und gibt Sicherheit für die nächsten Schritte – und sollte einer nach dem anderen dokumentiert werden. Sie werden sehen, es bildet sich rasch ein beachtlicher Bestand an dokumentierten Datenschutzmeilensteinen heraus.

Tipp 6: Inzwischen existiert auf den verschiedenen Ebenen (Europa/Bund/Länder) eine Vielzahl von Informationen zu allen relevanten Datenschutzthemen – man muss diese nur finden und dieses Wissen einfach verfügbar machen. Es kann daher helfen, die **Informationsflüsse zu steuern** und regelmäßig die Stellungnahmen des Europäischen Datenschutz-Ausschusses, die Entscheidungen des Europäischen Gerichtshofes, die Dokumente der Deutschen Datenschutzkonferenz oder die Empfehlungen der Landesbeauftragten nachzuverfolgen. So entsteht nach und nach ein Wissens- und Erfahrungsschatz, auf den man dann in künftigen Situationen zurückgreifen kann. Man muss lediglich seine Informationsquellen finden und dann regelmäßig und systematisch nutzen.

Tipp 7: Ein vielfach vernachlässigter, aber datenschutzrechtlich zentraler Punkt ist die Erstellung eines **Löschkonzepts**, welches die relevanten Bereiche abdeckt und zu differenzierten, angemessenen Lösungen kommt. Allerdings weiß jeder, der sich etwas intensiver um diese Thematik gekümmert hat, dass sie äußerst vielschichtig ist und praktisch nur sehr schwer in den Griff zu bekommen ist. Mein Vorschlag: Auch hier empfiehlt es sich, Schritt für Schritt vorzugehen und so langsam und mit Ausdauer ein zusammenhängendes Konzept aufzubauen. Ziel kann hier nicht die Perfektion sein, Ziel ist es vielmehr, einen Anfang zu machen und das eigene Löschkonzept nach und nach zu verbessern.

III. Foreign Affairs

Tipp 8: Zusammen ist man weniger allein! **Netzwerke** helfen die relevanten Themen zu identifizieren, sich über Probleme auszutauschen und Hilfe für die eigene Tätigkeit zu bekommen. Nutzen Sie die immer zahlreicheren Angebote von Erfahrungsaustausch-Kreisen der betrieblichen Datenschutzbeauftragten – auch die Aufsichtsbehörden bieten immer mehr Fortbildungs- und Austauschmöglichkeiten an.

Tipp 9: Die **Beobachtung der Aufsichtsbehörden** lohnt sich nicht nur im Hinblick auf die dort bereitgestellten Informationen über datenschutzrechtliche Themen oder Dokumente, sondern auch im Hinblick auf die von ihnen gesetzten Schwerpunkte bei der Aufsicht, Kontrolle und Überprüfung. Heiße Kandidaten für künftige Prüfungen des LfDI Baden-Württemberg sind im 1. Halbjahr 2019 die Bestellung der betrieblichen Datenschutzbeauftragten und die Erfüllung der Informations- und der Dokumentationspflichten nach der DS-GVO. Fragen Sie bei Ihrer Aufsichtsbehörde nach, wo sie ihre Schwerpunkte bei Aufsicht und Kontrolle setzt.

Tipp 10: Schließlich sollten Sie auch den **„Feindkontakt“** suchen: Zögern Sie nicht, Anfragen an Ihre Datenschutz-Aufsichtsbehörde zu stellen, Ihre Lösungen uns zu präsentieren und mit uns zu diskutieren. Das zählt nicht nur zu den Pflichtaufgaben der Aufsichtsbehörden nach der DS-GVO – das hilft Ihnen bei der Erfüllung Ihrer anspruchsvollen und umfangreichen Arbeit für den Datenschutz mit Sicherheit weiter!

Über den Autor

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

▶ www.baden-wuerttemberg.datenschutz.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg

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

Datenschutz Know-how seit 1996

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

DATENSCHUTZ IN KMU UND VEREINEN

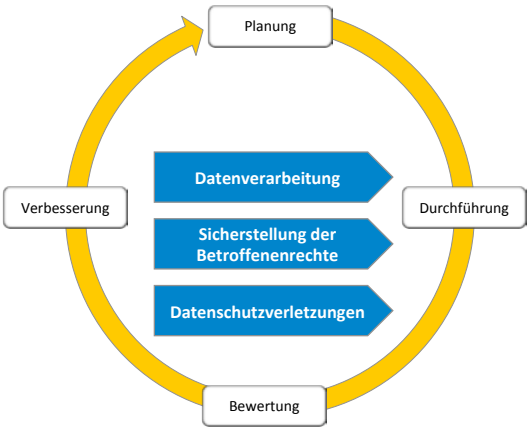
Thomas Kranig

Die ab dem 25. Mai 2018 anwendbare Datenschutz-Grundverordnung (DS-GVO) sah in der Entwurfsfassung der Kommission noch die eine oder andere Erleichterungsregelung für KMUs vor, die im Zuge des Gesetzgebungsverfahrens im Ergebnis verloren gegangen sind. Dies bedeutet, wenn man sich den in Art. 2 DS-GVO definierten sachlichen Anwendungsbereich anschaut, dass die DS-GVO für den Handwerksbetrieb und den Verein ebenso Anwendung findet wie für global agierende Unternehmen, die auf dem europäischen Markt ihre Geschäfte machen. Die Tatsache, dass die Rechtsvorschriften grundsätzlich gleichlautend anwendbar sind, bedeutet aber nicht, dass auch der Grad der Umsetzung für alle Verantwortlichen gleich ist. Für das konkrete Bemühen um Compliance, d. h. Einhaltung der Vorschriften, ist auf die konkrete Verarbeitungssituation abzustellen. Bei der Überlegung, was konkret zu machen ist, ist zu unterscheiden zwischen Aktivitäten, die jeder permanent machen muss und solchen, auf die man (nur) vorbereitet sein muss.

1. Permanent zu erbringende Aktivitäten

Permanent einzuhalten sind die Grundsätze für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO. Rechtmäßigkeit und Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit müssen in jedem Fall gegeben sein.

Dies klingt zunächst erschreckend umfangreich, kann sich aber, wenn man die konkrete Verarbeitungssituation zum Beispiel in einem Verein oder Handwerksbetrieb anschaut, als ziemlich überschaubar darstellen. Notwendig ist dabei, sich zunächst bewusst zu machen, wo der Datenschutz anfängt und wo er aufhört, d. h. wo personenbezogene Daten gemäß Art. 2 DS-GVO verarbeitet werden. Die in Art. 4 Nrn. 1 und 2 DS-GVO enthaltenen Definitionen können Vereinen und KMUs besser verständlich gemacht werden, wenn man sagt, dass „personenbezogene Daten" alle „Informationen sind, die irgendwie mit einer konkreten natürliche Person in Verbindung gebracht werden können" und „Verarbeiten" „alles ist, was man mit personenbezogenen Daten überhaupt machen kann".



Prüfen Sie bei Veränderung Ihrer Arbeitsweise, ob Ihre Datenschutzmaßnahmen noch passen und wirksam sind.

Permanent zu erbringen bedeutet dabei nicht, dass man täglich überprüfen muss, ob noch alles stimmt, sondern dass man die eigenen Anforderungen einmal ermittelt und umgesetzt haben und nur dann wieder anpacken muss, wenn im Umgang mit personenbezogenen Daten die Arbeitsweise geändert oder neue Zwecke erreicht werden sollen. Um erkennen zu können, welche

Anforderungen sich für den jeweiligen Verantwortlichen daraus ergeben, ist es notwendig, sich einen Gesamtüberblick darüber zu verschaffen, wer in welcher Art und Weise im „eigenen Laden" mit personenbezogenen Daten umgeht.

a) Grundsätze für die Verarbeitung personenbezogener Daten

Für einen Handwerksbetrieb stellen sich bei der Überprüfung der einzuhaltenden Grundsätze für die Verarbeitung personenbezogener Daten insbesondere folgende Fragen:

- **Rechtmäßigkeit und Transparenz**

  Darf ich die Daten meiner Mitarbeiter und meiner Kunden haben, die ich momentan von ihnen habe? Welche Daten habe ich aufgrund einer vertraglichen Beziehung, als Ergebnis einer für mich überwiegend positiven Interessenabwägung oder aufgrund einer Einwilligung? Wie werde ich die Daten, die ich gar nicht haben darf, wieder los?

- **Zweckbindung**

  Verwende ich die Daten meiner Mitarbeiter und meiner Kunden nur für zulässige Zwecke, z.B. zur Fortführung des Beschäftigungsverhältnisses und zur Pflege des eigenen Kundenverhältnisses?

- **Datenminimierung**

  Benötige ich die Daten, die ich habe oder in Zukunft erheben will, um den vorher benannten Zweck rechtmäßig erfüllen zu können oder speichere ich Daten nach dem „Grundsatz", „man weiß ja nie, wann mal die mal brauchen kann", was mit Datenminimierung nichts mehr zu tun hätte.

- **Richtigkeit**

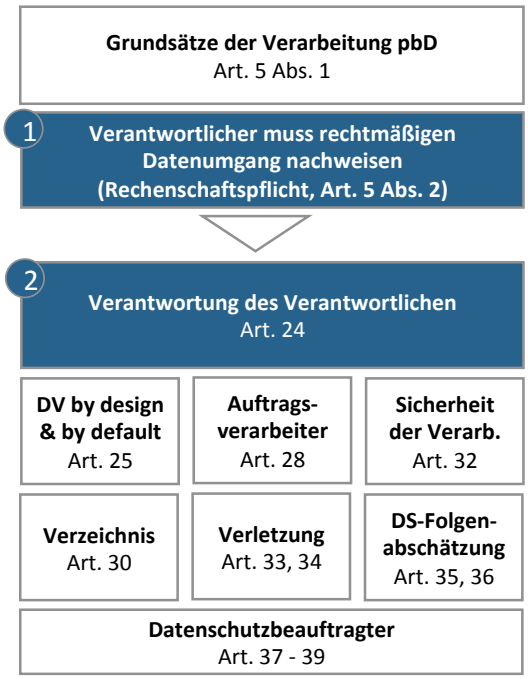
  Sind die Daten, die ich für die Erfüllung des vorher benannten Zwecks erforderlich sind, richtig?

- **Speicherbegrenzung**

  Brauche ich die Daten für die Erfüllung des vorher benannten Zwecks noch?

- **Integrität und Vertraulichkeit**

  Verarbeite ich die Daten meiner Mitarbeiter und meiner Kunden angemessen sicher?



b) Sicherstellung der Verantwortung

Ein Handwerksbetrieb oder auch ein Verein muss sich ferner die folgenden Themen bewusst machen und die daraus ergebenden Fragen für sich beantworten – und gegebenenfalls erforderliche Anforderungen umsetzen.

- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

  Eine hierbei zu stellende Frage: „Entwickle ich Produkte oder Projekte, bei denen ich mit personenbezogenen Daten umgehe, und wenn ja, habe ich dabei im Auge, diese so zu gestalten, dass der Schutz der personenbezogenen Daten meiner Mitarbeiter und meiner Kunden möglichst weitgehend gewahrt wird?" dürfte in aller Regel in dem hier angesprochenen Kontext kaum eine Bedeutung haben. Andererseits finden z.B. die Aktenvernichtung, ein Windows-Rollenkonzept, wie „nicht jeder verwendet die Administrator-Kennung" oder eine Datenschutzschulung der Mitarbeiter hier die rechtliche Grundlage.

- **Auftragsverarbeitung**

  Habe ich Aufgaben vergeben, bei denen mit personenbezogenen Daten umgegangen wird, zum Beispiel das Betreiben einer Webseite? Habe ich dafür eine entsprechende vertragliche Regelung?

- **Sicherheit der Verarbeitung**

  Welche personenbezogenen Daten verarbeite ich und habe ich insoweit angemessene Maßnahmen zum Schutz vor unbefugtem (z. B. Computer-Virus) oder unerwünschtem (z. B. Wasserschaden im Serverraum) Verhalten ergriffen?

- **Verzeichnis der Verarbeitungstätigkeiten**

  Habe ich ein Verzeichnis erstellt, in dem ich die wesentlichen Verarbeitungstätigkeiten dokumentiert habe?

- **Datenschutz-Folgenabschätzung**

  Es schadet nicht, zu wissen, dass es so etwas geben kann. Eine Relevanz für Verantwortliche im hier angesprochenen Kontext ist kaum vorstellbar.

- **Benennung eines Datenschutzbeauftragten**

  Sind bei uns ständig mindestens zehn Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt? Auch diese Voraussetzung dürfte im hier angesprochenen Kontext in den seltensten Fällen gegeben sein.

2. Bereit sein für anlassbezogene Aktivitäten

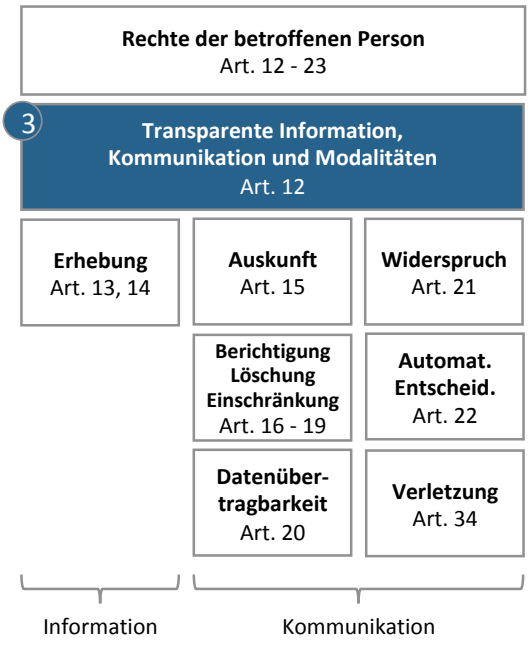
Neben den permanent zu erbringenden Aktivitäten müssen KMUs und Vereine auf besondere Ereignisse vorbereitet sein, die entweder von außen (Geltendmachung von Betroffenenrechten) oder von außen und von innen (Datenschutzverletzungen) eintreten können.

a) Geltendmachung von Betroffenenrechten

Abfragen bei größeren Informationsveranstaltungen für KMUs und Vereine haben ergeben, dass ein Anspruch auf Auskunftserteilung oder die Geltendmachung sonstiger Betroffenenrechte bisher fast nie vorgekommen sind. Entgegen der bisherigen Rechtslage, dass man dann, wenn ein entsprechender Anspruch geltend gemacht wurde, diesen („einfach nur") erfüllen musste, geht die DS-GVO insoweit ein Stück weiter, indem sie die Verantwortlichen verpflichtet, darauf vorbereitet zu sein (und dies nachweisen zu können), dass sie dann, wenn ein derartiger Anspruch kommt, diesen zeitnah erfüllen können. Für KMUs und Vereine bedeutet dies konkret, dass sie wissen müssen, welche Betroffenenrechte es gibt und einen – auch noch so einfachen – Plan haben müssen, wie damit umgegangen wird, wenn entsprechende Ansprüche geltend gemacht werden. Dieser Plan kann aber im einfachsten Fall als eine einseitige formlose Ergänzung zum Verarbeitungsverzeichnis umgesetzt werden.

Konkret bedeutet dies eine Vorbereitung auf die Geltendmachung eines Rechts auf

- Auskunft,
- Berichtigung, Löschung, Einschränkung,
- Widerspruch gegen Verarbeitungen auf Basis einer Interessenabwägung,
- Werbewiderspruch,
- Widerspruch gegen eine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung und
- Datenübertragbarkeit.



b) Meldungen von Datenschutzverletzungen

Ebenso wie für den Umgang mit den oben genannten Betroffenenrechten verpflichtet die DS-GVO den Verantwortlichen auch darauf, vorbereitet zu sein, dass Datenschutzverletzungen, d. h. Verletzungen der Verfügbarkeit, Vertraulichkeit und Integrität eintreten können. Dazu gehört auch, erkennen zu können, ob diese meldepflichtig sind oder nicht, und wenn ja, sie innerhalb von 72 Stunden der Aufsichtsbehörde zu melden. Auch hier gilt es, sich bewusst zu machen, dass es eine derartige Meldepflicht gibt und einen – auch noch so einfachen – Plan zu haben, wer in welcher Art und Weise handelt, wenn eine Datenschutzverletzung bekannt geworden ist. Dies beinhaltet auch, darauf vorbereitet zu sein, dass dann, wenn die Datenschutzverletzung zu einem hohen Risiko für die betroffenen Personen führt, diese angemessen informiert werden.

3. „Compliance-Checkliste“ für KMUs und Vereine

Jedes Unternehmen und jeder Verein ist unterschiedlich aufgestellt, so dass es eine Checkliste, die alle Konstellationen abdeckt, kaum geben kann. Die folgende Checkliste kann deshalb nur die regelmäßigen und wesentlichen Fragestellungen für KMUs und Vereine darstellen:

- Gibt es ein Bewusstsein bei Ihnen, dass „Datenschutz Chefsache ist“ und ist dieses Bewusstsein insoweit umgesetzt, dass sich jemand darum kümmert?
- Haben Sie Ihre Mitarbeiter belehrt und auf die Einhaltung des Datenschutzes verpflichtet?
- Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO?
- Haben Sie geprüft, ob Sie die Grundsätze der Verarbeitung personenbezogener Daten einhalten, d.h. u.a., ob Sie Daten, die Sie haben, haben dürfen? Haben Sie dabei geprüft, ob Sie für die Daten, die Sie nur auf der Basis einer Einwilligung verarbeiten dürfen, eine wirksame Einwilligungserklärung vorliegen haben?
- Haben Sie externe Dienstleister zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden? Wenn ja, haben Sie mit diesen einen entsprechenden Auftragsverarbeitungsvertrag mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?
- Wie kommen Sie Ihren Informationspflichten nach Artt. 13 und 14 DS-GVO nach? Haben Sie entsprechende Texte für die unterschiedlichen Kommunikationskanäle (Beitrittserklärung, Angebotserteilung, Internet) vorbereitet?
- Sind Sie darauf vorbereitet, Anträge auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch gegen Werbung oder gegen Verarbeitungen auf Basis einer Interessenabwägung, Widerspruch gegen eine ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung und/oder einen Antrag auf Datenübertragbarkeit innerhalb kurzer Zeit abarbeiten zu können?
- Haben Sie im Verhältnis zum Risiko für die Grundrechte der betroffenen Personen bei Ihrer Verarbeitung ausreichende technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus implementiert? Haben Sie sichergestellt, dass Datenschutzverletzungen bei Ihnen erkannt und sofern sie meldepflichtig sind, innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden?
- Haben Sie geprüft, ob Sie einen Datenschutzbeauftragten benennen müssen?

4. Fazit

Die DS-GVO ist ein Regelwerk für den Handwerksbetrieb und auch ein global agierendes Unternehmen. Ein Zweck der DS-GVO ist der Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen und damit von uns allen. Alle, die im Rahmen ihrer beruflichen Tätigkeit für einen Verantwortlichen handeln (Geschäftsführer, Inhaber, Mitarbeiter oder Vereinsvorstände usw.), gehen in dieser Funktion mit personenbezogenen Daten vieler anderer um, sind aber als natürliche Personen vielfach betroffene Personen zahlreicher anderer Verantwortlicher. Losgelöst von jeglicher gesetzlicher Verpflichtung sollten die für einen Verantwortlichen handelnden Personen so agieren, wie sie sich es als betroffene Person von den anderen Verantwortlichen wünschen.

Für Aufsichtsbehörden dürfte es Konsens sein, dass sie dann, wenn sie im Rahmen einer Beschwerde oder anlasslosen Prüfung auf einen Verantwortlichen stoßen, der sich um die Einhaltung der Datenschutzvorschriften bemüht, es ihm aber – aus Sicht der Aufsichtsbehörde – nicht oder nicht vollständig gelungen ist, diesem Verantwortlichen den „Weg zur Compliance“ zu weisen und ihn nicht mit einer Geldbuße zu bestrafen. Wer sich dagegen um Datenschutz gar nicht kümmert, hat bei Prüfung der Aufsichtsbehörde auf jeden Fall ein Problem.

Über den Autor

Thomas Kranig
Präsident des Bayerischen Landesamtes
für Datenschutzaufsicht

▶ www.lda.bayern.de

STRUKTURELLE SCHWÄCHEN DES EU CYBERSECURITY ACTS – GRUNDSÄTZLICHE HERAUSFORDERUNGEN BEI DER REGULIERUNG VON IT-SICHERHEIT

Jan-Peter Kleinhans

Im September 2017 hat die Europäische Kommission den Entwurf eines Rechtsaktes zur Cybersicherheit[1] vorgelegt – der Trilog wird mit großer Wahrscheinlichkeit schon im Winter 2018 abgeschlossen sein. Mit besagtem Rechtsakt zur Cybersicherheit (CSA)[2] versucht die EU zum ersten Mal ein Rahmenwerk für die Entwicklung einheitlicher Anforderungen an die IT-Sicherheit von Produkten und Diensten im Binnenmarkt zu etablieren. Die Schnelligkeit und Intensität mit der in Brüssel über den Rechtsakt verhandelt wurde, legt zumindest die Vermutung nahe, dass Kommission, Parlament und Rat von der grundsätzlichen Notwendigkeit und Dringlichkeit gleichermaßen überzeugt waren. Erklärtes Ziel ist zum einen durch einheitliche Standards und Zertifizierung Transparenz über die Vertrauenswürdigkeit von Produkten und Diensten zu schaffen. Zum anderen sollen Unternehmen langfristig einen Mehrwert darin sehen ihre Produkte nach Europäischen IT-Sicherheitsanforderungen zertifizieren zu lassen, um so einen Wettbewerbsvorteil zu erlangen – der Markt für zertifizierte Produkte soll also gestärkt bzw. überhaupt erst erschaffen werden.

Mit dem CSA setzt die EU auf das Zusammenspiel aus Standardisierung und Konformitätsbewertung bzw. Zertifizierung, um IT-Sicherheit im EU Binnenmarkt zu stärken. Dieser Ansatz ist gut und richtig, birgt jedoch speziell bei IT-Si-

[1] EU Kommission. 2017. COM(2017)477/947932. Proposal for a Regulation. https://ec.europa.eu/info/law/better-regulation/initiative/1090/publication/111956/attachment/090166e5b5ae9e12

[2] Cybersecurity Act, CSA

cherheit mehrere Herausforderungen, die durch den CSA adressiert werden müssten:

1. Zertifizierung als Momentaufnahme

Wird ein Produkt durch ein unabhängiges Prüflabor gegen definierte IT-Sicherheitsanforderungen zertifiziert oder durch eine Konformitätsbewertungsstelle die Konformität zu bestimmten Normen bescheinigt, handelt es sich hierbei immer lediglich um eine Momentaufnahme. Gerade bei vernetzten Produkten, deren Funktionalität zu einem Großteil durch Software definiert wird, „altert" eine solche Überprüfung nur sehr schlecht: Wie viel Aussagekraft hat eine Zertifizierung basierend auf Softwareversion 1.1 des Produktes, wenn es ein halbes Jahr später bereits mit der Softwareversion 1.7 ausgeliefert wird? Die *Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)*, eine der wenigen IT-Sicherheitsnormen mit internationaler Relevanz, haben beispielsweise damit zu kämpfen, dass Unternehmen eine Re-Zertifizierung aufgrund des hohen Zeit- und Kostenaufwandes meist scheuen.[3] Ergebnis ist, dass zertifizierte Produkte unter Umständen weniger häufig aktualisiert werden. Da der CSA selbst dieses Spannungsverhältnis *zwischen einmaliger Produktzertifizierung und konstanter Softwareentwicklung nicht auflöst*, liegt die Verantwortung nun bei den Gremien, die für die Entwicklung der zukünftigen Europäischen Zertifizierungsschemata zuständig sind. Es braucht effektive und effiziente Ansätze[4], um die Aussagekraft von Zertifikaten über einen substanziellen Teil der Produktlebenszeit zu erhalten.

2. Selbsterklärung benötigt Marktüberwachung

Der CSA erlaubt es Herstellern selbst zu bescheinigen, dass ein Produkt konform zu Europäischen IT-Sicherheitsstandards ist. Der Hersteller muss also nicht erst ein externes Prüflabor mit der Konformitätsbewertung beauftragen, sondern kann eine simple Selbsterklärung abgeben, dass sich bei der Entwicklung an die jeweiligen Standards gehalten wurde. Beim CSA ist eine solche Selbsterklärung nur bei Produkten mit „niedriger" Vertrauenswürdigkeitsstufe möglich – welche Geräte unter welchen Bedingungen als „niedrig" eingestuft werden, muss noch definiert werden. Das System der Selbsterklärung ist beispielsweise bei der CE-Kennzeichnung (physische Produktsicherheit) etabliert und gibt letztlich Herstellern einen „Vertrauensvorschuss", um zügig und kostengünstig Produkte am Markt zu veröffentlichen. IT-Produkte sind schnelllebig und der Markt ist hoch-innovativ, daher ist es verständlich, dass die EU auch beim CSA Herstellern die Möglichkeit geben will, Zeit und Kosten einer externen Konformitätsbewertung zu sparen. Allerdings hätte man von der CE-Kennzeichnung lernen sollen: Es gibt Hersteller, die den „Vertrauensvorschuss" einer Selbsterklärung ausnutzen und nicht-konforme Produkte auf den Markt bringen – diese müssen durch eine effiziente und effektive nachgeschaltete Marktüberwachung identifiziert und deren Hersteller sanktioniert werden.

Die Marktüberwachung für die CE-Kennzeichnung hat mit einigen Problemen[5] zu kämpfen, doch leider wurde aus diesen Erfahrungen, zumindest bei der Entwicklung des CSA, nicht gelernt. Stattdessen findet man faktisch keine Aussagen zur Marktüberwachung im CSA. Ebenso wurde die Frage der Sanktionierung von Herstellern bei Fehlverhalten auf die Mitgliedsstaaten abgewälzt. Dies birgt das Risiko einer heterogenen Sanktionslandschaft innerhalb Europas. Letztlich unternimmt der CSA keinerlei Anstrengungen Marktüberwachung für IT-Sicherheit zu modernisieren und zu stärken. Ganz im Gegenteil, aus den Herausforderungen der CE-Kennzeichnung wurde nichts gelernt und somit besteht die reale Gefahr, dass Hersteller die Freiheiten der Selbsterklärung ausnutzen, um ungestraft nicht-konforme Produkte zu veröffentlichen. Dies wiederum wird das Vertrauen der Verbraucher in die IT-Sicherheit von Produkten am EU Binnenmarkt erodieren.

3. Entkoppelt von restlicher Standardisierung in Europa

Der CE-Kennzeichnung liegen dutzende EU Produktsicherheitsrichtlinien zugrunde, die Anforderungen an Produkte definieren. Im Zuge des *New Legislative Frameworks*[6] hat die EU eine relativ klare Rollenverteilung bei der Technologieregulierung aufgestellt: Der Gesetzgeber definiert Regulierungsziele und die drei ▶

[3] Jan-Peter Kleinhans. 2018. „Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit". Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf

[4] Jan-Peter Kleinhans. 2018. „Improving IoT security in the EU: Why pre-market certifcation is not enough and how to fix it". Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/european_iot_product-database.pdf

[5] Algemene Rekenkamer. 2017. „Products sold on the European market: unraveling the system of CE marking". https://english.rekenkamer.nl/publications/reports/2017/01/19/products-sold-on-the-european-market-unraveling-the-system-of-ce-marking

[6] Europäische Kommission. „New Legislative Framework". https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en

europäischen Normungsorganisationen (CEN, CENELEC, ETSI) entwickeln anschließend gemeinsam mit der Industrie Standards (beispielsweise besagte Produktsicherheitsrichtlinien für die CE-Kennzeichnung), die konform mit den Regulierungszielen sind. Hersteller von Produkten bescheinigen durch die Konformität zur jeweiligen Richtlinie somit automatisch auch die Konformität zur übergeordneten Regulierung. Dadurch will die EU vermeiden technische Anforderungen in Gesetze zu schreiben, da diese bekanntlich sehr schlecht altern. Weiterhin sind die Normungsorganisationen den *Grundprinzipien der Normung*[7], aufgestellt durch die Welthandelsorganisation, verschrieben und die Standardisierungs- und Normungsarbeit ist auf nationaler, europäischer und internationaler Ebene koordiniert.

Obwohl der CSA das New Legislative Framework referenziert und Konzepte, wie die Selbsterklärung, daraus nutzt, ist man bei der Entwicklung und Verabschiedung der zukünftigen europäischen IT-Sicherheitsstandards bzw. -zertifizierungsschemata einen eigenen Weg gegangen: Statt die Normungsorganisationen mit der Entwicklung zu betrauen, wurden eigene, neue Gremien geschaffen, in denen den nationalen Sicherheitsbehörden der Mitgliedsstaaten (BSI, ANSSI, etc.) zentrale Bedeutung zukommt. Da die Zertifizierungsschemata des CSA nicht nur für Konsumgüter relevant sein sollen, sondern auch Standards für kritische Infrastrukturen entwickelt werden sollen, ist es verständlich, dass nationale Sicherheitsbehörden der Mitgliedsstaaten hier stärker involviert sein möchten – zumal sie eine hohe fachliche Kompetenz haben. Gleichzeitig ist durch das Erschaffen paralleler Strukturen bei der Standardisierung bisher ungeklärt, wie zukünftige europäische IT-Sicherheitsstandards des CSA in den internationalen Standardisierungsorganisationen gespiegelt werden. Ebenso muss abgewartet werden, wie transparent die Entwicklung der europäischen Zertifizierungsschemata in den neuen Gremien abläuft.

Fazit

Regulierung (mit dem Ziel der nachhaltigen Stärkung) von IT-Sicherheit ist schwierig und der Teufel steckt oft im Detail. Umso wichtiger ist es von anderen Bereichen, beispielsweise der Regulierung physischer Produktsicherheit, zu lernen und Fehler nicht zu wiederholen. Der Rechtsakt zur Cybersicherheit ist ein wichtiger und guter erster Schritt, um IT-Sicherheit im europäischen Binnenmarkt langfristig zu stärken. Auch der Fokus auf Standardisierung und Zertifizierung ist verständlich und richtig. Jedoch wurde es versäumt von den Problemen der CE-Kennzeichnung und der nachgeschalteten Marktüberwachung zu lernen. Zunächst wurde unterschätzt, dass die drei Elemente Standardisierung, Konformitätsbewertung bzw. Zertifizierung und Marktüberwachung gleichermaßen berücksichtigt und gestärkt werden müssen: Während der CSA der Entwicklung der Standards (Zertifizierungsschemata) viel Aufmerksamkeit schenkt, wird die zwingend notwendige Marktüberwachung und Sanktionierung bei Fehlverhalten bzw. Nicht-Konformität faktisch vollständig ignoriert. Weiterhin wurde verkannt, dass eine einmalige Produktzertifizierung mit jedem Software-Update an Aussagekraft verliert. Dadurch, dass der CSA lediglich ein Rahmenwerk schafft, um Anforderungen an die IT-Sicherheit von Produkten und Diensten innerhalb Europas überhaupt zu definieren, bleibt zu hoffen, dass einige der Schwächen bei der späteren Entwicklung der tatsächlichen Zertifizierungsschemata noch nachgebessert werden können.

Über den Autor

Jan-Peter Kleinhans
Projektleiter IT-Sicherheit
im Internet der Dinge
Stiftung Neue Verantwortung e.V., Berlin

[7] Welthandelsorganisation. 2013. „International Standards And The Wto Tbt Agreement: Improving Governance For Regulatory Alignment". https://www.wto.org/english/res_e/reser_e/ersd201306_e.pdf

VOM DATENSCHUTZ ZUR HUMAN-ZENTRIERTEN DATENWIRTSCHAFT

Malte Beyer-Katzenberger

Wenn Tim Berners-Lee, einer der „Erfinder" des World Wide Web, spricht, dann hört die (Netz-) Gemeinde zu. So geschehen am 29. September 2018 in einem Interview mit dem Onlinemagazin Fast Company.[1] Es geht darin um nichts Geringes als das Bemühen, das Web wieder zu dem zu machen, was es ursprünglich war: Ein dezentral organisiertes peer-to-peer Netzwerk. Die Macht der Plattformen, die sich als Gatekeeper im Netz etabliert haben, soll zurückgedrängt werden. Wir alle sollen die Kontrolle über unsere Daten wiedererlangen. Inrupt[2] – nicht ‚disrupt', der so populäre Terminus für die radikale Erneuerung eingespielter Geschäftsmodelle durch die neuen digitalen Möglichkeiten: Der Name ist Programm. Ein wenig überwältigend war offenbar die Resonanz: In der englischsprachigen Medienlandschaft fand die Vorstellung grosses Echo. Ein Team-Mitglied berichtete auf Twitter von über tausend Emails, die nach der Veröffentlichung des Interviews eingegangen seien.

Auch nach der öffentlichen Ankündigung bleiben gewisse Unklarheiten, was Solid[3], die zugrunde liegende Technologie, und Inrupt, der Versuch darauf kommerzielle Dienste anzubieten, genau sind und welches Geschäftsmodell sicherstellt, dass sich das Modell am Markt behauptet. Bekannt ist lediglich, dass im Herzen des Projektes ein „personal online data store", sitzt, ein vom Einzelnen kontrollierter Speicherplatz. Unklar bleibt, ob die Datenspeicherung lokal oder in einer Cloud erfolgt – oder ob das dem Nutzer überlassen wird. Rund um diesen personal online data store sollen dann Entwickler Apps anbieten.

Bemerkenswert ist, dass es eine ganze Reihe ähnlicher Ansätze schon seit geraumer Zeit gibt. Eine ganze Reihe von Start-ups sind seit Jahren in Europa (und anderswo) unterwegs und bieten in etwa dasselbe – mit Unterschieden in den technischen Lösungen (Datenspeicherung in eigener oder fremder Cloud, komplett dezentralisierte Systeme ohne „personal data store") und im Geschäftsmodell (kooperative Formen, Finanzierung durch Transaktionsgebühren ähnlich den Kreditkartenunternehmen oder monatliche Festpreise für angeschlossene Unternehmen). Sie heissen digi.me, CozyCloud, meeco, Fair & Smart, Hub-of-all-things, Mydex, Qiy Foundation oder Health Bank Cooperative, um nur einige zu nennen. Sie haben gemeinsam Prinzipien einer human-zentrierten Datenwirtschaft formuliert[4] und sich jüngst am 11. Oktober 2018 zu einer MyData genannten Organisation zusammengeschlossen.

Das Potenzial wurde erkannt: Schon 2014 machte die spezialisierte britische Beratungsfirma Ctrl+Shift einen kommenden Markt für solche neuartigen, Personal Information Management Services' mit einem Volumen von GBP 16,5 Mrd (Euro 18,5 Mrd) aus[5]. Die Stiftung Datenschutz hat die rechtlichen, technischen und ökonomischen Dimensionen 2016/17 in einer dreiteiligen Studie eingehend untersuchen lassen.[6]

Dennoch warten alle diese Projekte bislang auf den grossen Durchbruch. Warum könnte jetzt der Zeitpunkt gekommen sein, wo solche Bemühungen Realität werden? Fünf Aspekte sind zu nennen: (1) Eine steigende Unzufriedenheit mit dem Geschäftsgebaren etablierter Akteure im Lichte wiederkehrender Enthüllungen; (2) ein im Lichte von Big Data und Künstlicher Intelligenz weiter wachsender Datenhunger gepaart mit dem Bemühen es datenschutzrechtlich „richtig" zu machen; (3) das Vorhandensein aller für eine Selbstkontrolle der Daten notwendigen technischen Mittel (ubiquitäre Internetkonnektivität, Akzeptanz und Nutzung von Cloudlösungen durch Verbraucher, zufriedenstellende Rechnerleistung auch auf Smartphones und Tablets); (4) die beginnende Verbreitung intelligenter Maschinen, gerade auch im Haushalt, die zu einer Vermehrung der Datenerzeugung, u. U. in Echtzeit, führen wird; die Organisation dieses Datenstroms stellt neue Herausforderungen; (5) nicht zuletzt die Regeln der Datenschutz-Grundverordnung, insbesondere die gesteigerten ▶

[1] JHttps://www.fastcompany.com/90243936/exclusive-tim-berners-lee-tells-us-his-radical-new-plan-to-upend-the-world-wide-web

[2] https://www.inrupt.com/

[3] https://solid.inrupt.com/how-it-works

[4] http://mydata.org

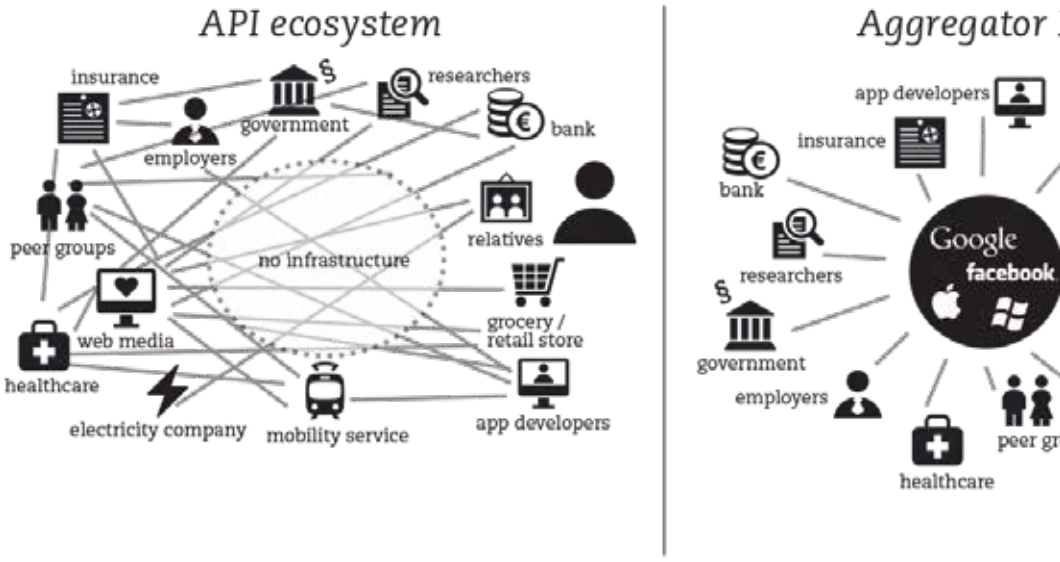
[5] https://www.ctrl-shift.co.uk/insights/2014/06/16/personal-information-management-services-an-analysis-of-an-emerging-market/

[6] https://www.stiftungdatenschutz.org/themen/pims-studie/

Anforderungen an die Einwilligung und das neue Portabilitätsrecht aus Artikel 20, welche in praktisch allen Unternehmen Umdenkungsprozesse im Datenmanagement hervorgerufen haben.

Der erste Schritt sind web-basierte Dashboards, mit denen eine mittlerweile steigende Zahl von Unternehmen den Nutzern ihrer Dienste ermöglicht, die Nutzung ihrer personenbezogenen Daten genauer zu steuern. Das kann aber nur der Anfang sein. Angesichts der Ubiquität der Datenerhebung bei Online-Diensten wird ein System, in dem der Nutzer auf u. U. Dutzenden von Online-Diensten jeweils gesondert die Datennutzungsoptionen einstellt, praktisch an seine Grenzen stossen. Und das ist nicht nur aus der Nutzerperspektive mühselig. Unternehmen, die neue Dienste auf der Grundlage von Big Data Analytics oder Künstlicher Intelligenz anbieten wollen, bleiben gezwungen, Daten über Datenbroker hinter dem Rücken der Betroffenen zu erstehen. Das bleibt unbefriedigend trotz aller Bemühungen, die diese Datenbroker unternehmen, um robuste Mechanismen zum Datenschutz zu entwickeln.

In letzter Konsequenz muss es möglich werden, die Daten wieder an ihrer Quelle, also beim Individuum abzuholen. Aus einer an den Bedürfnissen von Organisationen ausgerichteten Datenwirtschaft wird eine human-zentrierte Datenwirtschaft. Ganz gleich, ob der Einzelne seine Daten virtuell in einem personal data store ablegt oder ob er in einem trust framework von kompatiblen Organisationen den Datenaustausch zwischen zwei Organisationen über ein web-basiertes Dashboard selbst steuern kann: Die Datenwirtschaft sollte den Einzelnen in den Mittelpunkt stellen.[7] Das Schaubild zeigt das hier befürwortete Modell im Vergleich zu zwei anderen Szenarien für die Datenwirtschaft.



Quelle: Poikola, Kuikkaniemi, Honko, MyData – A Nordic Model for human-centered personal data management and processing."

Interessanterweise machen es gerade genossenschaftlich organisierte Unternehmen vor, dass ein solcher Ansatz möglich ist: Die französische MAIF Versicherungsgruppe und die finnische Einzelhandelsgenossenschaft S-Group bieten ihren Kunden die Visualisierung und Mitnahme ihrer Daten über Programmierschnittstellen an. Datenportabilität wird praktische Wirklichkeit.

Daraus könnten sich ganz neuartige Dienste entwickeln: Personal Big Data heisst das Stichwort. Dabei sollen nicht Muster aus der massenhaften Analyse von Daten über eine Vielzahl von Personen entdeckt werden, sondern Korrelationen zwischen Datenbeständen über ein und dieselbe Person. Aus der Kombination von Daten aus Fitnesstrackern, über Einkaufsverhalten und über Umwelteinflüsse können relevante Informationen zur Verbesserung des Lebensstils gezogen werden. Mangels Zugang zu einer Vielzahl von Datenquellen sind solche Dienste heute nur sehr schwer möglich.

[7] Siehe hierzu das illustrative finnische MyData Konzept: https://www.lvm.fi/documents/20181/859937/MyData-nordic-model/

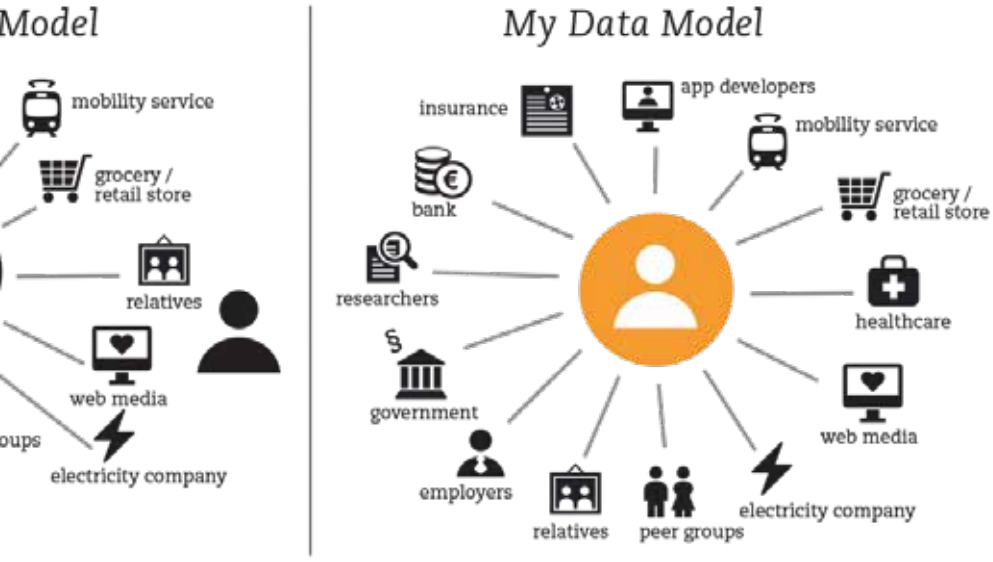
Was ist zu tun?

Die Datenschutz-Grundverordnung enthält wichtige Bausteine eines human-zentrierten Internets, allen Voran das Auskunfts- und das Portabilitätsrecht sowie das Einwilligungserfordernis für bestimmte Situationen, insbesondere bei der Nutzung sensibler Daten. Die Übersetzung in die Architektur der Datenverarbeitung in Unternehmen ist im Gange, wird aber an manchen Stellen, insbesondere hinsichtlich der Ermöglichung von Datenportabilität, noch Zeit brauchen. Unternehmen sind hier gefordert, die Datenverarbeitung auch vom Nutzer her zu denken und ihm/ihr auch in technischer Hinsicht die bestmöglichen Kontroll- und Mitnahmemöglichkeiten zu geben.

Die Europäische Kommission unterstützt die Idee eines human-zentrierten Internets.[8] Sie fördert weitere technische Entwicklungen finanziell im Rahmen ihrer Initiative „Next Generation Internet"[9] und „Building a European data economy".[10]

Die Idee einer stärkeren Verantwortung des Einzelnen durch Daten"selbstverwaltung" birgt evident Gefahren. Sie muss daher weiter eingehegt bleiben durch ein Datenschutzrecht, das effektiv durchgesetzt wird, insbesondere durch staatliche Aufsichtsbehörden aber ergänzt durch kollektiven Rechtsschutz[11]. Darüber hinaus beginnt eine Debatte über Eingrenzung der Datennutzung, insbesondere im Kontext der Anwendung künstlicher Intelligenz (Datenethik). Deutschland und andere EU-Mitgliedstaaten haben hierzu Diskussionsprozesse in Gang gebracht.

Es wird deutlich, dass sich die Struktur der Datenwirtschaft hinsichtlich personenbezogener Daten grundlegend verändern könnte und ein neuer Typus von Informationsintermediären entstehen kann. Mögliche Monopolisierungstendenzen könnten so aufgelöst werden und der Wettbewerbsdruck auf die Entwicklung des überzeugenderen Dienstes oder der überlegenen technischen Lösung hin verlagert werden.



Ministry of Transport and Communications, 2015]

Über den Autor

Malte Beyer-Katzenberger
ist Referent bei der Europäischen Kommission, Generaldirektion Kommunikationsnetzwerke, Inhalte und Technologien (Connect) und arbeitet zu Grundsatzfragen der Datenwirtschaft. Er gibt lediglich seine persönliche Auffassung und nicht die der Europäischen Kommission wieder.

[8] Bruno Kessler Vorlesung des Generaldirektors von DG CONNECT, Roberto Viola, vom 30. Juli 2017 https://ec.europa.eu/digital-single-market/en/news/internet-humans-how-we-would-internet-future-be

[9] www.ngi.eu

[10] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/ict-13-2018-2019.html

[11] Siehe Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Verbandsklagen zum Schutz der Kollektivinteressen der Verbraucher vom 11.4.2018.

FULL HOUSE FÜR BESSEREN DATENSCHUTZ

BvD-Herbstkonferenz 2018

BvD und die Datenschutzaufsichtsbehörden aus Baden-Württemberg und Bayern luden unter dem Motto „Wirtschaft trifft Aufsicht" zur 2. Herbstkonferenz nach Stuttgart.

Schon der Zuspruch ließ ahnen: Die Herbstkonferenz vom 24. bis 25. Oktober 2018 in Stuttgart mit dem anschließenden Behördentag am 26. Oktober 2018 kann nur ein Erfolg werden.

Für die ersten beiden Konferenztage, die unter dem Motto „Wirtschaft trifft Aufsicht" standen, hatten sich über 250 Teilnehmer angemeldet. Betriebliche und behördliche, externe und interne Datenschutzbeauftragte, Mitarbeiterinnen aus Datenschutz-Abteilungen, Fachleute aus den Aufsichtsbehörden, aus Ministerien und Fachreferaten diskutierten über die Umsetzung der Datenschutz-Grundverordnung (DS-GVO) und die Probleme, die sich nach rund 150 Tagen seit Gültigwerden zeigen. Eines der heißen Themen: Die Bestrebungen der Landesregierungen in Bayern und Baden-Württemberg, die Benennungspflicht für Datenschutzbeauftragte nach § 38 BDSG n.F. zu lockern.

Schon bei der Eröffnung am Mittwoch im voll besetzten Saal des Hotels Steigenberger Graf Zeppelin machte sich BvD-Vorstandsvorsitzender Thomas Spaeing über die Debatte zur Benennungspflicht Luft: „Ohne den betrieblichen und behördlichen Datenschutzbeauftragten kann der Mittelstand Datenschutz nicht umsetzen", sagte er. Denn ohne das Datenschutz-Knowhow wisse niemand in den Unternehmen, was sie überhaupt tun müssten.

Spaeing weiß, dass viele kleine und mittlere Unternehmen (KMU) sich mit der Datenschutz-Grundverordnung schwer tun. Aber gerade jene, die sich bislang noch gar nicht mit der DS-GVO beschäftigten, forderten jetzt die Lockerung der Benennungspflicht, kritisierte er.

> *„Wir sind in Deutschland beim Datenschutz gut aufgestellt. Aus dem Ausland schauen sie zu uns und sagen: ‚Die haben es richtig gemacht'. Aber jetzt ist die Politik dabei, dieses Ansehen zu verspielen, zu Lasten von Betroffenen, Verbrauchern und Bürgern."*
> *(Thomas Spaeing, BvD-Vorstandsvorsitzender)*

Spaeing sieht aber auch Lücken in der Aufklärung zur DS-GVO. „Wenn beim Bäcker oder Friseur Formulare zur Einwilligung der Datenerhebung ausliegen, dann läuft etwas schief." Informationslücken hätten der Skandalisierung und Panikmache Raum gegeben." Dabei seien auf der Grundlage der DS-GVO neue Unternehmenszweige, Rechenzentren und Start-Ups entstanden, für die der europäische Datenschutz ein Alleinstellungsmerkmal im internationalen Geschäft ist.

Stefan Brink: „Bleiben Sie mutig“

Dr. Stefan Brink, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, unterstrich bei der Eröffnung, vor allem die KMU hätten Probleme bei der Umsetzung der DS-GVO. Im Gesetzestext sei versäumt worden, etwa bei den Dokumentationspflichten, zwischen Konzernen und Kleinunternehmen zu unterscheiden. „Daraus ist eine negative Stimmung gegen den Datenschutz entstanden“, sagte er. Aber, ob die EU-Verordnung im Zuge eines Reformprozesses das hinbekomme, darüber zeigte sich Brink skeptisch. „Ich befürchte, dass wir das nicht in den nächsten zehn Jahren erleben werden.“

Die über 250 Teilnehmer rief er auf, in den Unternehmen und Behörden für einen guten und praktikablen Datenschutz einzutreten. „Bleiben Sie mutig“, sagte er, „entwickeln Sie eigene Ansätze und Lösungen.“ Denn Datenschutz habe in Deutschland eine lange Tradition. „Das sollte uns selbstbewusst genug machen.“

Thomas Kranig, Präsident des Bayerischen Landesamts für Datenaufsicht, ermutigte den BvD, sich stärker auf europäischer Ebene einzubringen und die Reformprozesse langfristig zu begleiten. Sein Wunsch: „Dass wir ins Gespräch kommen, welche praktischen Anwendungen funktionieren, welche überzogen sind und wie sie für verschiedene Unternehmens- und Organisationsformen praktikabel umsetzbar sind.“

Saskia Esken: DSB sind ein „absoluter Aktivposten“

Mit der netzpolitischen Sprecherin der SPD-Bundestagsfraktion, Saskia Esken, hatte sich die Herbstkonferenz eine überaus kompetente Politikerin für die Key-Note ins Haus geholt.

Für sie sind die Datenschutzbeauftragten ein „absoluter Aktivposten“ im europäischen Datenschutz. Denn sie sicherten die Verbraucher- und Datenschutzrechte bei der Verarbeitung personenbezogener Daten. „Wenn kein Vertrauen in die Digitalisierung vorhanden ist, dann gehen uns die Menschen von der Fahne“, warnte sie. Schon jetzt sei Datenschutz für viele zum „Kampfbegriff“ geworden. Dagegen müssten Politik und Verbände gleichermaßen antreten.

Unter anderem regte Esken die Stärkung der Datenschutzkonferenz sowie eine bessere personelle Ausstattung der Aufsichtsbehörden in den Ländern an. Auch beim Beschäftigtendatenschutz müsse die große Koalition endlich vorankommen, mahnte sie.

Eine Lockerung der Benennungspflicht für DSB lehnt Esken ab. Es sei eine Fehleinschätzung zu glauben, wenn ein Unternehmen keinen DSB benennen müsse, bräuchten sie auch keinen Datenschutz umzusetzen. „Wir haben in Europa die Chance, beim Datenschutz einen ganz eigenen Weg zu gehen“, sagte sie. Diese Chance dürfe jetzt nicht verspielt werden.

Von Hackern lernen: Workshops und Live-Hacking

Der Nachmittag des ersten Konferenztags und der Vormittag des zweiten Tages boten viele parallele Sessions, auch das neue Format „Die Datenschutz-Aufsichtsbehörde beantwortet Ihre Fragen“, die von Stefan Brink und seinem Team initiiert wurde.

Außerdem gab es gleich drei Live-Hacking-Demonstrationen von Thomas Floß und seinem Mitarbeiter Sebastian von der Au sowie von Sebastian Schreiber.

Schreiber simulierte unter anderem einen Angriff auf einen Web-Shop, auf eine Funk-Alarmanlage und wie man mit einfacher Software SMS fälschen kann. Thomas Floß und Sebastian von der Au zeigten, wie sich Passwörter und WhatsApp-Nachrichten knacken lassen und wie eine Malware per USB-Stick das Antiviren-Programm umgeht.

Weitere Workshops widmeten sich unter anderem den Themen Privacy Litigation, Datenschutz in Bewerbungsverfahren, aktuelle Löschsysteme und wie gründlich sie sind, technischer Datenschutz, die Umsetzung der DS-GVO in einem internationalen Unternehmen, Fanpages bei Facebook sowie Umsetzung von Betroffenenrechten.

▶

Premiere Behördentag

Eine Premiere feierte der Behördentag, der sich am Freitag an die beiden ersten Konferenztage anschloss. Rund 150 Datenschutzexperten aus Verwaltung und Ämtern waren nach Stuttgart gekommen, um sich über spezielle Fragen zum Datenschutz in der Verwaltung auszutauschen.

Der stellvertretende BvD-Vorstandsvorsitzende Jürgen Hartz betonte in seiner Begrüßung, Behörden hätten im Zuge der DS-GVO bislang weniger im Fokus der öffentlichen Debatten gestanden. Dabei seien die Anforderungen auch bei ihnen hoch. „Ämter und Verwaltungen stehen vor den gleichen Herausforderungen wie die Wirtschaft", sagte er. Bürgerinnen und Bürger erwarteten aber gerade von Verwaltungen beim Thema Datenschutz Vertrauen und Sicherheit.

Für Stefan Brink war es auch Ziel dieses ersten Behördentags, den DSB in den Amtsstuben mehr Selbstbewusstsein und Wertschätzung mit auf den Weg zu geben. „Machen Sie genau das, was Sie für richtig halten", ermutigte er die Teilnehmenden, „gehen Sie mit Energie und Überzeugung an ihre Aufgabe".

> *„Uns ist bewusst, dass der Datenschutz im öffentlichen Sektor nicht nur auf offene Türen stößt. Aber im Sinne der informationellen Selbstbestimmung der Bürger können die Datenschutzbeauftragten in den Behörden selbstbewusst die neuen Anforderungen angehen."*
> *(Dr. Stefan Brink, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg)*

Am Ende zeigten sich die drei Veranstalter von den drei konzentrierten Konferenztagen begeistert. „Wir sind fest entschlossen, das Format auch weiterhin zu unterstützen", versicherte Brink zum Abschluss.

Die Vorträge und Referate der Workshops sind auf bvdnet.de unter der Rubrik „BvD-Herbstkonferenz" nachzulesen.

▶ https://www.bvdnet.de/bvd-herbstkonferenz-datenschutz-2018/

SAVE THE DATE:

Die nächste Herbstagung findet vom 23.-25. Oktober 2019 in Nürnberg statt.

Erhitzte Gemüter: Ministerialrat Will (BayStMI) stellt sich der BvD-Herbstkonferenz in Stuttgart

Schon nach wenigen Minuten fühlte sich BvD-Vorstandsvorsitzender Thomas Spaeing verpflichtet, eine sachliche Diskussion anzumahnen. Das war nötig, denn in Saal 8 des Stuttgarter Hotels Steigenberger Graf Zeppelin, in dem am 24. und 25. Oktober die zweite BvD-Herbstkonferenz stattfand, hatte sich Michael Will den Datenschutzbeauftragten gestellt.

Michael Will ist Ministerialrat im Bayerischen Innenministerium. Bayern und Baden-Württemberg hatten im Bundesrat eine Initiative eingebracht, die die bisherige Benennungspflicht für DSB auflösen will. Sein Argument: Die Bestellpflicht ist nicht mehr zeitgemäß und belaste kleine und mittlere Unternehmen (KMU). Stattdessen setzt sein Haus auf Selbstregulierung.

Die Initiative wurde im Oktober 2018 von der Länderkammer abgelehnt, aber „die Debatte geht weiter", kündigte Will an und spekuliert auf eine entsprechende gesetzliche Änderung im Zuge der Novelle des neuen Bundesdatenschutzgesetzes zum Frühjahr 2019. Davor soll es eine neuerliche Sachverständigenanhörung geben.

Spaeing hatte im Sommer an einem ersten „Round-Table-Gespräch" teilgenommen und für die Beibehaltung der bestehenden 10-Personen-Regel geworben. „Wenn es keine Pflicht mehr zum Datenschutzbeauftragten gibt, dann gibt es auch keinen Datenschutz mehr bei den Firmen", fasste er die Bedenken in Stuttgart zusammen. Mit einer konzertierten Kampagne arbeitet der BvD weiter daran, die Benennungspflicht für Unternehmen mit zehn Personen und mehr in der Datenverarbeitung zu erhalten.

Dass Will mit der bayerischen Position für Unmut unter den etwa 150 Teilnehmenden sorgte, die sich in Saal 8 drängten, überraschte wenig. Er selbst war auf Gegenwind eingestellt. „Ich habe den Fluchtwagen vor der Tür stehen", scherzte er und sorgte damit wenigstens für einen Moment der Auflockerung.

Denn klare Worte bekam er auch von den Aufsichtsbehörden aus Bayern und Baden-Württemberg, die gemeinsam mit dem BvD zur Herbstkonferenz nach Stuttgart eingeladen hatten, mit auf den Weg.

Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg, betonte, der Datenschutz in Deutschland funktioniere im Wesentlichen über den betrieblichen und behördlichen Datenschutzbeauftragten (DSB). Sie seien absolut essentiell. „Wer daran sägt, sägt am Datenschutz-Niveau in Deutschland", argumentierte er. Da seien sogar die Aufsichtsbehörden selbst „eher verzichtbar" als die DSB.

Zwar sind die Aufsichtsbehörden über die DS-GVO abgesichert, fügte Thomas Kranig hinzu, Präsident des Bayerischen Landesamts für Datenschutzaufsicht. Die interne Kontrolle sei mit den DSB in Unternehmen und Verwaltungen aber wesentlich besser geworden. Zudem habe Deutschland in Europa den Datenschutzbeauftragten durchgesetzt. Insofern sei er froh, dass die Bundesratsinitiative gescheitert sei.

Will selbst versuchte am Ende zu beruhigen: Mit dem Blick auf die Selbstregulierung werde die Expertise der DSB nicht unnötig. Die Verantwortlichen in den Unternehmen bräuchten diese auch weiterhin. Das sei ähnlich wie bei der Unternehmens-Beratung, argumentiert er, stellte aber auch klar: Eine „Zwangsberatung" wolle er nicht mehr.

Ein neues Format für Fragen aus der Praxis

„Die Datenschutz-Aufsichtsbehörde beantwortet Ihre Fragen" hieß das neue Format, das der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg auf der zweitägigen BvD-Herbstkonferenz in Stuttgart anbot – mit überwältigendem Erfolg.

An den beiden Sessions auf der Herbstkonferenz, die unter dem Motto „Wirtschaft trifft Aufsicht" stand, nahmen jeweils fast ein Drittel der über 250 Kongress-Teilnehmenden teil - trotz harter „Konkurrenz" von parallelen Sessions. Am zweiten Tag wechselte das Fachteam aus Stuttgart sogar den Raum, damit mehr Teilnehmende unterkamen. Aber auch dieses Mal mussten viele wieder stehen.

Die Fragen waren so vielfältig wie die Tätigkeit der Datenschutzbeauftragten: Es kamen Fragen nach der Arbeit des europäischen Datenschutzausschusses und der deutschen Datenschutzkonferenz, nach der Unterstützung bei der Entwicklung von Codes of Conduct, nach Informationspflichten und Zweckbestimmungen bei der Datenerfassung, nach Zertifizierungen und Akkreditierungen, nach einer sicheren Anonymisierung von Daten, nach Meldepflichten bei Risikofolgenabschätzung und Datenpannen und auch danach, ob ein externer Datenschutzbeauftragter seine Kunden ausschließlich telefonisch beraten darf.

Die Mitarbeiter der Datenschutzaufsicht von Baden-Württemberg hatten die Fragen im Vorhinein erhalten und dann aus ihrer Sicht rechtsgültige Antworten erarbeitet. Dabei berührten sie auch Themen wie die Verarbeitung personenbezogener Daten in der Fotografie oder die Einbindung der virtuellen Amazon-Assistentin Alexa in eine Kunden-App.

Mitunter suchten die Experten der Datenschutzaufsicht Baden-Württemberg griffige Beispiele für ihre Erläuterungen. Auf die Frage, wie die Datenverarbeitung bei der Einbindung etwa von Ehrenamtlern in ein Projekt geregelt werden könne, führten sie die vier Biberbeauftragten in Baden-Württemberg an, die bei ihrer Arbeit unter anderem personenbezogene Daten von Grundstückseingentümer erhalten. Die Antwort: Auch Biberbeauftragte sind auf Geheimhaltung zu verpflichten - etwa in einem Werkvertrag, der explizit auf die Datenschutzbestimmungen verweist.

Den baden-württembergischen Datenschutzbeauftragten Stefan Brink freute die Nachfrage nach dem neuen Format. „Auch wenn wir viele Beratungen anbieten. Die Zahl der auf der Tagung eingereichten Fragen hat uns doch überrascht", sagte er der BvD-News. Auf der Herbstkonferenz 2019 soll es das Format wiedergeben.

BvD-News: Christina Denz

MIT HUMOR FÜR DEN DATENSCHUTZBEAUFTRAGTEN KÄMPFEN

Cartoon-Serie

Die aktuelle Diskussion über die mögliche Lockerung der Benennungspflicht für Datenschutzbeauftragte (DSB) und die vor allem vom Bundeswirtschaftsministerium angestrebte Änderung von § 38 Abs.1 BDSG beschäftigt den BvD seit Monaten.

Zur Unterstützung unserer politischen Arbeit, bei der wir für den Erhalt der jetzigen 10-Personen-Regel eintreten und auch die Öffentlichkeit für das Thema sensibilisieren wollen, haben wir in Zusammenarbeit mit dem Zeichner und Karrikaturisten Alff drei Cartoons aufgelegt.

Sie setzen mit Humor unsere Position um, wonach eine Lockerung oder gar Abschaffung der Benennungspflicht nur vordergründig kleinen und mittleren Unternehmen etwas bringen würde. Tatsächlich sinkt durch das mangelnde Know-how das Datenschutzniveau und die Gefahr für höhere Bußgelder durch die Aufsichtsbehörden steigt eklatant.

„Kein Unternehmen ist in der Lage, ohne fachliche Expertise zum Beispiel die geforderte Datenschutz-Folgenabschätzung zu erstellen", kritisierte BvD-Vorstand Thomas Spaeing auf der zweiten Herbstkonferenz in Stuttgart, auf der wir die Motive vorstellten. Vielmehr sind es die Datenschutzbeauftragten, die maßgeblich dafür sorgen, dass der Datenschutz in den Unternehmen funktioniert.

Die rund 250 Teilnehmenden der zweitägigen Herbstkonferenz, die unter dem Motto „Wirtschaft trifft Aufsicht" stand, erhielten die Motive als Poster. Wer nicht dabei war, kann sie als Download auf https://www.bvdnet.de/humor/ herunterladen und zur Visualisierung in der Debatte um den Erhalt der Benennungslpflicht verwenden. Eine kommerzielle Nutzung ist ausgeschlossen.

Machen Sie mit und unterstützen Sie unsere Arbeit für den Erhalt von § 38 Abs.1 BDSG – damit das erfolgreiche deutsche DSB-Modell weiter als Vorbild für Europa dienen kann.

Informationen über die Aktivitäten des BvD in der politischen Diskussion sowie Handlungsempfehlungen, wie kleine und mittelständische Unternehmen entlastet werden können, ohne die Benennungspflicht zu verändern, finden Sie auf www.bvdnet.de und https://www.bvdnet.de/themen/dsb/.

Über den Autor

Jürgen Hartz
Stellv. Vorstandsvorsitzender des BvD e. V.

DATENSCHUTZ GERAPPT

Ein Blick hinter die Kulissen

„Was die App so macht, wird am Anfang kurz erwähnt, doch dann ist es schon zu spät, Deine Daten unterwegs", singt Kevin Lehmann in einem Studio im ehemaligen Kreuzberger Umspannwerk mitten in Berlin. Er steht an einem heißen Augustwochenende vor der Kamera von Regisseur Holger Eggert für ein professionelles Video zu seinem selbst komponierten Rap-Song „Datenschutz".

Der 18-Jährige aus Oldenburg hatte 2017 den „Sonderpreis Jugend" beim ersten Datenschutz Medienpreis (DAME) des BvD mit dem Song gewonnen. Die Jury aus Datenschutz- und Medienexperten war davon so begeistert, dass die europäische Datenschutz-Initiative klicksafe.de spontan 500 Euro für den Sonderpreis stiftete. Mit Unterstützung der DATEV-Stiftung Zukunft hat der BvD in diesem Sommer ein Musik-Video zum Song erstellt. Das Ziel: Junge Leute für die komplexen Themen rund um den Datenschutz gewinnen.

Als Komparsen sind mehrere Berater-Scouts dabei, die wie Kevin Lehmann für den Verein JUUUPORT ehrenamtlich Jugendliche beraten, die Opfer von Mobbing oder Abzocke im Internet werden. Außer in Kreuzberg drehte das Film-Team noch in der BvD-Geschäftsstelle, am Alexanderplatz und auf dem Gelände des Velodrom im Prenzlauer Berg. Kevin Lehmann singt an diesem Wochenende seinen Song mindestens 50 Mal.

„Die zwei Drehtage haben mir extrem Spaß gemacht und ich bin glücklich, dass so ein cooles Video herausgekommen ist." sagt er. „Cool", das ist so ein Wort, das häufiger während des Drehs fällt. Die jungen Leute von JUUUPORT e.V. sind begeistert von den Szenen, die Regisseur Holger Eggert mit ihnen für das Musik-Video durchgeht – und natürlich auch davon in Berlin einen Clip zu drehen.

Beim Dreh mit dabei: BvD-Mitglied Ralf Heimburger, der sich im Arbeitskreis Schule und in der Initiative „Datenschutz geht zur Schule" engagiert, macht sich als Beleuchter verdient. Katrin Eggert von der Geschäftsstelle sorgt für Requisite, Make-Up und Verpflegung.

„Es ist schön zu sehen, dass Datenschutz nicht nur eine Sache von Fachleuten und engagierten Verbrauchern ist, sondern die jungen Leute genauso umtreibt", sagt Heimburger. „Und das in so einem coolen Rhythmus."

Ralf Heimburger ist seit Jahren mit der Initiative „Datenschutz geht zur Schule" in Oberstufenzentren, Sekundarstufen und Grundschulen unterwegs. „Im praktischen Leben spielt Datenschutz für die Jugendlichen eine enorme Rolle", sagt er. „Denn sie nutzen ganz selbstverständlich und ständig die neuen Medien – und sind damit den Gefahren aus dem Internet um so mehr ausgesetzt."

BvD-Vorstandsvorsitzender Thomas Spaeing betont, „vor allem die jungen Leute sind es, die oft unter Datenmissbrauch leiden. Deshalb ist es wichtig, eine Sprache und ein Medium zu finden, mit dem wir die Jugendlichen erreichen."

Nach Schnitt und Postproduktion steht das Video seit dem 26. September 2018 auf YouTube – und bekam allein schon am ersten Tag über 1.000 Klicks. Zu finden ist es auf YouTube ▸

unter den Stichworten „Kevin Lehmann“ und „Datenschutz“.

Das Musikvideo „Datenschutz“ wird vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit (TLfDI) für den Einsatz an Thüringer Schulen im Thüringer Schulportal (TSP) aufgenommen und wird durch das

Thüringer Lehrerfortbildungsinstitut (ThILLM) kostenfrei zum Download in der Mediothek des TSP zur Verfügung gestellt

(https://www.schulportal-thueringen.de/media).

Die DAME des BvD: Bewerbungsschluss für zweite Runde

Für die zweite Runde des mit 3.000 Euro dotierten DAME-Hauptpreises, für den gerade die Bewerbungsfrist endete, haben Filmschaffende, Journalisten, Video-Künstlerinnen und Engagierte aus dem gesamten deutschsprachigen Raum fast 40 Clips, Erklärfilme, Animationsproduktionen, Musikvideos, Reportagen und Sartirebeiträge eingereicht. Die DATEV-Stiftung Zukunft, die seit 2015 „Datenschutz geht zur Schule“ fördert, ist auch als Sponsor bei DAME 2018/Preisverleihung 2019 dabei.

Bei der ersten Preisverleihung (DAME 2017) im April 2018 zeigte sich die Jury begeistert über die Bandbreite der Einreichungen: Viele Beiträge erklärten Datenschutz anschaulich und verständlich, manche witzig, manche provokant. Die Bewerbungen der zweiten Runde erweitern diese Bandbreite noch.

Die Jury sichtet nun bis Ende des Jahres die Beiträge und diskutiert darüber, wie die Bewerber die Qualitätskritierien für anschauliche und verständliche Erklärungen umgesetzt haben. Im Februar 2019 wird sie drei Nominierte bekannt geben, die zur Preis-Gala im Rahmen der BvD-Verbandstage 2019 am 5. Juni nach Berlin eingeladen werden. Dort wird TV-Moderator Ralph Caspers wieder den oder die Gewinner „DAME 2018“ in einer feierlichen Preisverleihung bekannt gegeben.

BvD-News: Christina Denz, Katrin Eggert

DOZENTENTAG 2018

Initiative Datenschutz geht zur Schule (DsgzS)

Es ist schon eine schöne Tradition geworden: Im Herbst werden die aktiven Dozenten der Initiative „Datenschutz geht zur Schule" eingeladen zusammenzukommen und rund um datenschutz- und medienpädagogische Themen einen fachlichen Austausch durchzuführen. Ermöglicht wird dies der Initiative durch eine großzügige Förderung durch die DATEV-Stiftung Zukunft. Dieses Jahr unterstütze der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg durch Referenten und bei der Organisation einer Schule für einen Aktionstag. Insgesamt zehn Referenten reisten schon einen Tag früher an und konnten so an der Eichendorf-Schule ca. 250 Schülerinnen und Schüler zum verantwortungsbewussten Umgang mit eigenen und fremden Daten sensibilisieren. Es war diesmal sogar möglich sich gegenseitig zuzuhören und so Anregungen zum eigenen Vortrag zu erhalten. Am Nachmittag gab es für die Dozenten eine interessante und anschauliche Führung zu Stuttgarts großem Bauprojekt Bahnhof 21 unter dem Stichwort „S21 erleben". Bei dem Dozentenstammtisch, einem gemeinsamen Abendessen wurde dann Kraft für die Vorträge am eigentlichen Dozententag getankt.

Mit Gästen von drei Aufsichtsbehörden, 17 Dozentinnen und Dozenten sowie mehreren externen Referenten (also insgesamt knapp über 30 Teilnehmenden) konnte ein fachkundiges Publikum von den Vorträgen zu datenschutz- und medienpädagogische Themen profitieren.

Miriam Ruhenstroth stellte mobilsicher e.V. vor, der zu einem sicheren und vertrauensvollem Umgang mit mobilen Geräten berät und informiert. Dazu werden beispielsweise nicht nur regelmäßig YouTube –Tutorials veröffentlicht, sondern auch Apps getestet. Den Zuhörerinnen und Zuhörern konnten frische Testergebnisse präsentiert werden: welche Daten sendet die App TikTok (vormals Musical.ly) beim Aufrufen weiter? Gibt es eine Möglichkeit, dies zu kontrollieren oder überhaupt wahrzunehmen? Wie geht man gegen einen Anbieter vor, der in Hongkong sitzt? Sehr schnell war die fachkundige Zuhörerschaft in ▸

die Diskussion eingebunden.

Am Beispiel der Suchmaschine „FragFinn“ erläuterte die Medienpädagogin Melanie Endler anschließend die Zielsetzung und die Umsetzungsmöglichkeiten, ein kindgerechtes Angebot im Internet zu platzieren. FragFinn wird getragen von Unternehmen und Verbänden der Medienbranche, die inhaltlich keinen Einfluss nehmen, aber ein Eigeninteresse daran haben, dass das Medium Internet auch der Zielgruppe der Minderjährigen ein adäquates Angebot bietet.

Martin Dörr und Alvar Freude vom LfDI Baden-Württemberg stellten dann am praktischen Beispiel „Einsatz von Mobile Devices im Schulunterricht und die Verwendung privater Datenverarbeitung bei den Lehrkräften“ dar, wie sich die aktuelle Situation in Baden-Württemberg gestaltet: Lehrern wird gestattet, private Hard- und Software einzusetzen, wenn sie sich verpflichten, dabei festgelegte Standards einzuhalten. Dabei gibt es nicht nur Definitionsprobleme („aktuelle Software“), auch eine rechtskonforme abgesicherte elektronische Kommunikation scheitert oftmals an technischen Kenntnissen bei mindestens einem der Kommunikationspartner.

Prof. Holger Nohr von der Hochschule der Medien in Stuttgart stellte die Ergebnisse und Ansätze der Regulierung des Datenschutzes für Kinder vor. Die Hochschule für Medien bietet mit dem „Master of Media Research“ einen bundesweit einmaligen „Forschungsmaster“ an. Dabei werden im Rahmen an der Arbeit am eigenen Forschungsprojekt auch Projekte zum Datenschutz thematisiert und erforscht wie z. B. das Datenschutzbewusstsein bei der social-media-Nutzung von Kindern und Jugendlichen oder „Brauchen wir ein Recht auf Dateneigentum“. Anhand von Beispielen aus der KIM-Studie 2016 legte er dar, wie weit die Angaben der Eltern zur Freigabe von Social-Media-Diensten zu der durch Befragungen festgestellten Realität abweichen. Ausführungen zur Kinderrechtskonvention der UN und der Umsetzung des Kinderschutzes in der DS-GVO rundeten den Vortrag ab.

Den Anwesenden wurde durch die klicksafe-Mitarbeiterin Stefanie Rack die gemeinsam überarbeitete Auflage des Lehrerhandouts zu den Vorträgen von „Datenschutz geht zur Schule“ vorgestellt. Aussagen wurden dabei an die DS-

GVO angepasst, der Teil Cybermobbing wurde zugunsten eines Kapitels über Selbstdarstellung ersetzt und die Ausgabe um Arbeitsblätter „Datensatz – Datenschatz“ sowie „Drohnen“ergänzt. Voraussichtlich im Dezember 2018 wird dann die dritte Auflage in gedruckter Fassung vorliegen.

Im abschließenden Austausch konnten dann auch unter Einbeziehung der Einschätzung der Vertreter der Aufsichtsbehörden aktuelle Fragestellungen zur Umsetzung der DS-GVO oder zu Datenschutz-Managementsystemen diskutiert werden. Aufgrund dieser interessanten Vorträge und Themen und dem regen Austausch untereinander verging der Tag wie im Flug. Wir danken an der Stelle auch dem Team des LfDI Baden-Würtemberg für die Unterstützung vor Ort. Umso schöner, dass wir schon jetzt wissen, dass auch im Jahr 2019 ein Dozententag stattfinden wird.

BvD-News: Rudi Kramer

DATENSCHUTZ-GRUNDVERORDNUNG

Ehmann / Selmayr (Hrsg.)

Die 2. Auflage des Kommentares zur Datenschutz-Grundverordnung aus dem C.H. Beck-Verlag liegt vor. Besonderen Augenmerk verdient die Aufnahme der Anpassungs- und Durchführungsgesetze von Deutschland (BDSG) und Österreich (DSG).

Die nationalen Ergänzungsregelungen BDSG und DSG fließen bei der Kommentierung der einschlägigen Bestimmungen der Datenschutz-Grundverordnung ein und werden aus europarechtlicher Sicht kritisch bewertet.

Die Neuauflage berücksichtigt außerdem die aktuelle Rechtsprechung des EuGH sowie die Evaluierung des EU-US Privacy Shields. Berichtungen der DS-GVO vom Mai 2018 wurden ebenfalls berücksichtigt.

Die 1. Auflage aus 2017 war bereits ein vielseitiges Werk, dessen Umfang und Tiefe den Anforderungen gerecht wurde. Mit den Ergänzungen, Kommentaren und praxisnahen Hinweisen, Erörterungen von Begrifflichkeiten in der 2. Auflage wird eine wertvolle Hilfe geleistet, ohne die bisherige deutsche Rechtsentwicklung zu vernachlässigen.

Der Kommentar zeichnet sich durch eine klare Struktur und Systematik aus, was das Arbeiten mit dem Werk zu einer Freude macht. Ein Auffinden der einschlägigen Fragen wird erleichtert, kombiniert mit einer kompakten, aufschlussreichen und leicht verständlichen Kommentierung, auch bei komplexen Fragestellungen. Ergänzt wird dies durch entsprechende Hinweise auf die nationalen Datenschutzgesetze Deutschlands und Österreichs.

Mein Resümee: Höchst lesenswert und empfehlenswert - gehört in das Bücherregal eines jeden Datenschutzbeauftragten.

Ehmann / Selmayr (Hrsg.)
»DATENSCHUTZ-GRUNDVERORDNUNG«

C. H. Beck Verlag

2. Auflage 2018
1.132 Seiten
ISBN 978-3-406-72006-2
149,00 Euro

Rezension von

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

▶ www.AdOrgaSolutions.de

DS-GVO UND EPRIVACY AUF WEBSITES UMSETZEN

Kristin Benedikt / Alexander Buckel / Jan-Hendrik Mammen

Die drei Autoren sind als Referenten bzw. Referatsleiterin einer deutschlandweit beachteten Datenschutzaufsichtsbehörde bekannt. Ihr dortiges Aufgabengebiet umfasst die technischen und rechtlichen Fragestellungen rund um den Betrieb einer Webseite.

Allein dieses Hintergrundwissen macht neugierig auf das Werk, das selbst keine offizielle Publikation der Aufsichtsbehörde darstellt. Als Zielgruppe werden nicht unbedingt DSB angesprochen, sondern Webmaster, Developer und Designer, Marketing- und IT-Mitarbeiter und Blogger. Angesichts der Reaktionen und (oftmals erwartungskonformen) Meinungsäußerungen aus diesen Gruppen aus Anlass der Anwendbarkeit der DS-GVO eine dankbare Zielgruppe, die sich um Verantwortliche in Vereinen und Unternehmen erweitern lässt.

In 10 Kapiteln werden in Fragen und kurzen Antworten alle denkbaren Konstellationen aufgeführt. Neben den Grundlagen, der Datenschutzerklärung, dem Kontaktformular, Analytics vs. Tracking, der Sicherheit, Newsletter, Social Media, Drittinhalte, werden auch Fragen zum Online-Shop, Content Management System und Web-App und Mobile Response behandelt. Mit über 250 Fragen werden dabei Aspekte aus dem Alltag behandelt. Man ahnt, dass hinter vielen Fragen konkrete Beratungsanlässe der Aufsichtsbehörde stehen, dementsprechend fundiert und belastbar erscheinen die Antworten.

Die Fragen und Antworten verwenden Fachbegriffe, bleiben aber auch für den „Datenschutzeinsteiger" leicht verständlich. Die Antworten werden jeweils den Kategorien Recht, Information, Nutzer und Sicherheit zugeordnet. Bei Recht erfolgt ein Verweis auf die heranzuziehende rechtliche Norm. Die Kapitel werden flankiert durch eine Handlungsfigur, die als neuer Mitarbeiter eines Unternehmens als Webmaster eingesetzt wird und dadurch mit verschiedenen Themen konfrontiert wird. Die abgehandelten Fragen umfassen alle Bereiche, die einem auch „im wirklichen Leben" begegnen. Die Antworten sind kurz und prägnant, ohne dass etwas ausgelassen wird.

Es eignet sich für den Einsteiger wie für erfahrene Datenschutzbeauftragten, denen es auch genügt, ihren Wissensstand zu überprüfen oder dem privat bloggenden aber datenschutzkritischem Kollegen auch mal zitierfähige Fundstellen zu zeigen, die niedrigschwellig genug formuliert sind, um auch da verstanden zu werden. Ein Ausblick zum rechtlichen Umfeld rundet das Werk ab.

Beigefügte Muster für eine Information nach Art. 13 DS-GVO sowie eines Fensters zur Einwilligung zum Cookie-Einsatz helfen bei der praktischen Umsetzung.

Es ist uneingeschränkt empfehlenswert für alle, die eine rechtskonforme Webseite betreiben möchten oder dazu beraten.

Benedikt / Buckel / Mammen
»DS-GVO und ePrivacy auf Websites umsetzen«

Verlag: Independently published

1. Auflage, Oktober 2018
296 Seiten
ISBN-13: 1720199472
Preis: 14,95

DATENSCHUTZ IN BAYERN

Wilde / Ehmann / Niese / Knoblauch

Wilde / Ehmann / Niese / Knoblauch
»Datenschutz in Bayern«

Rehm Verlag, München

29. Aktualisierung, Stand Juni 2018
ISBN-13: ISBN 978-3-7825-0353-2
Loseblattwerk 169,99 €
Vierteljahrespreis 49,99 Euro
Aktualisierung ca. 2 mal im Jahr
auch als Onlineprodukt erhältlich

Die Autorenschaft setzt sich aus renommierten, auch über Bayern hinaus bekannten, Experten zusammen und wurde mit der 29. Aktualisierung um Dr. Schwabenbauer erweitert.

Der Aktualisierungslieferung umfasst den Gesetzestext der DS-GVO und des BayDSG. Ferner werden in dem Teil der „Weiteren Vorschriften" relevante Bundesgesetz wie die Abgabenordnung, Sozialgesetzbuch I und X, aber auch Landesgesetze wie das Bayerische Erziehungs- und Unterrichtsgesetz aktualisiert.

Die Kommentierung beschreibt anschaulich die verschiedenen Bereiche, die durch das BayDSG abgedeckt werden und gibt konkrete Anwendungshinweise.

Angereichert wird die Kommentierung durch tabellarische Übersichten, wie bspw. zu dem in Art. 11 BayDSG geregelten Datengeheimnis über institutionelle Verschwiegenheitspflichten im Bayerischen Landesrecht.

Auch wenn im BayDSG - wie im BDSG auch - Regelungen enthalten sind, bei denen bereits jetzt schon die entsprechende Gesetzgebungskompetenz angezweifelt wird (wie bei den Vorgaben zur Videoüberwachung in § 4 BDSG), erfolgt die Kommentierung dazu ausführlich und differenziert, mit Ausführungen, die auch bei Überlegungen zur Auslegung des § 4 BDSG verwendet werden können.

Zu erwähnen ist noch, dass das Werk von einem Newsletter begleitet wird, in dem aktuelle Informationen vermittelt werden.

Anwender des Bayerischen Datenschutzrechts werden nicht umhinkommen, sich mit diesem Standardwerk auseinander zu setzen. Aber auch darüber hinaus bieten die Kommentierungen Hilfestellungen und Anregungen für vergleichbare Formulierungen und Sachverhalte aus der DS-GVO.

ANTWORTEN FÜR DIE PRAXIS: DATENSCHUTZ IN DER BETRIEBSRATSARBEIT

Torsten Lemken

Torsten Lemke
»Antworten für die Praxis: Datenschutz in der Betriebsratsarbeit«

Verlag Vahlen (C.H. Beck), München

64528 Seiten
ISBN: 978-380064834
16,90 Euro

Der Autor ist als Rechtsanwalt im Kollektivarbeitsrecht und dabei insbesondere in der Beratung von Betriebsräten auch zu datenschutzrechtlichen Fragestellungen tätig. Die dabei gewonnene Erfahrung zeigt sich auch in der Struktur und Aufbau des Ratgebers, der in der Reihe „Arbeitshilfen für Betriebsräte" erscheint. Insgesamt 125 Fragen werden in den 9 Kapiteln behandelt. Hierbei geht es um Mitbestimmung des Betriebsrates beim Datenschutz, die Kontrolle durch den Betriebsrat, die Datenverarbeitung durch den Betriebsrat, den Beschäftigtendatenschutz, die Datenauswertung durch den Arbeitgeber, externe Services und Auslandsbezug im Datenschutz, Details zu einzelnen IT-Anwendungen, der Abschluss von Betriebsvereinbarungen und die DS-GVO im allgemeinen.

Ein Stichwortregister hilft zu einzelnen Themen die Fragestellungen zu finden. Anhand der Auswahl der Fragestellungen ist der Praxisbezug des Autors erkennbar. Die Fragen und Antworten werden niedrigschwellig aufbereitet, spezielles Vorwissen ist nicht erforderlich. Zu vielen Punkten werden Praxistipps und Beispiele ergänzt.

Am Ende der Arbeitshilfe finden sich 14 Muster beispielsweise für Einwilligungen nach Art. 7 DS-GVO, Musterbriefe des Betriebsrats, Checklisten für den Abschluss von Betriebsvereinbarungen wie zum IT-Einsatz oder einer Videoüberwachung aber auch einem Verzeichnis der Verarbeitungstätigkeiten.

Insgesamt ist diese Arbeitshilfe ein übersichtlicher und konkreter Ratgeber nicht nur für Betriebsräte, sondern auch für Datenschutzbeauftragte, die sich mit Fragen zum Beschäftigtendatenschutz befassen und konkrete Antworten bevorzugen.

LEITFADEN ZUR DATENSCHUTZ-GRUND-VERORDNUNG - UMSETZUNGSHILFEN FÜR DIE PRAXIS

Lepperhoff / Müthlein (Hrsg)

Lepperhoff / Müthlein (Hrsg)
»Leitfaden zur Datenschutz-Grundverordnung - Umsetzungshilfen für die Praxis«

Datakontext, München

2. Auflage
528 Seiten
ISBN: 978-3-89577-820-9
44,99 Euro

Die beiden Herausgeber muss man in Datenschutzkreisen nicht weiter vorstellen. Gemeinsam mit vielen weiteren Experten, die sich aus Praxisberatern, Autoren und Referentinnen bei unterschiedlichen Landesdatenschutzaufsichtsbehörden zusammensetzen, haben sie die 2. Auflage als Umsetzungshilfe der gesetzlichen Anforderungen geschaffen. Beiträge aus Fachzeitschriften wurden zusammengestellt, überarbeitet und aktualisiert. Leider fehlt eine Zuordnung der einzelnen Beiträge zu den im Werk aufgeführten mitwirkenden Autoren.

Das Werk gliedert sich in 10 Teile, die insgesamt 41 Themenfelder darstellen. Neben der Einleitung, der Rechenschaftspflicht zur Dokumentation, der Arbeit des Datenschutzbeauftragten, dem Spezialgebiet der Werbung, den Betroffenenrechten, der Auswirkung auf die Personalwirtschaft, den Auswirkungen auf die IT-Administration und die IT-Sicherheit, der Auftragsverarbeitung und Softwareanbieter, der Compliance-Kosten vs. Nutzen und zum Schluss dem Umgang mit Altverhältnissen finden sich die wesentlichen Fragestellungen systematisch dargestellt.

Das Werk eignet sich gut für den Einstieg in die Thematik, insbesondere, wenn man die Darstellung zu konkreten Themen sucht. Gerade für den Überblick aber auch das Verständnis bei komplexeren Fragestellungen sind die eingesetzten Checklisten und Infografiken hilfreich. Angesichts der Spannbreite der Themen, die behandelt werden, werden bei zahlreichen speziellen Fragen weitere Werke herangezogen werden müssen. Schließlich haben auch die Aufsichtsbehörden zu einigen Themen schon Kurzpapiere verfasst, die ergänzend hinzugezogen werden können. Gleichwohl bietet der Leitfaden eine ausreichende Grundbasis, sich mit der DS-GVO auseinanderzusetzen.

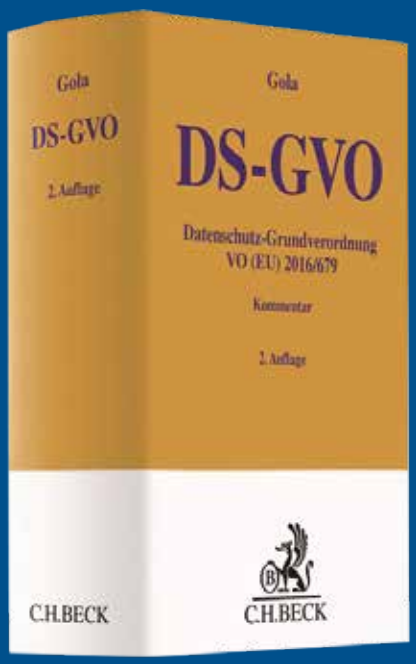
Die Grafiken im Buch sind für den Nutzer nach Registrierung über einen Content-Code auch online zugänglich.

Rezensionen von

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

DATENSCHUTZ-GRUNDVERORDNUNG: DS-GVO VO (EU) 2016/679

Peter Gola



Peter Gola
»Datenschutz-Grundverordnung: DS-GVO VO (EU) 2016/679«

C.H.BECK

2. Auflage 2018
1.092 Seiten
ISBN 978-3-406-72007-9
85,00 Euro

Der Kommentar von Gola zum alten BDSG im gleichen Format konnte unumwunden als einer der Standardkommentare zum BDSG bezeichnet werden. Der nunmehr in der 2. Auflage vorliegende Kommentar zur Datenschutz-Grundverordnung knüpft hier an.

Der eigentlichen Kommentierung der einzelnen Artikel der DS-GVO ist eine Einführung von Herrn Prof. Gola sowie der Gesetzestext vorangestellt. Das macht den Kommentar zu einem in der Praxis autonom nutzbaren Werk. Die Einführung und die sehr praxisnahe Kommentierung der Regelungen eignen sich hervorragend für den Einstieg. Die Einleitung als bloßen Einstieg zu bezeichnen, täte dieser jedoch unrecht.

Denn sie verdeutlicht grundlegende Aspekte,

die für das Verständnis und die Auslegung der DS-GVO insgesamt bedeutend sind (ein Beispiel ist die mit „Ein Stück Datenschutz-Flickenteppich bleibt“ überschriebene Zusammenstellung der Öffnungsklauseln). Die Qualität und die Detailierung der praxiserfahrenen Autoren lässt aber auch die Vertiefung der Fragestellungen zu. Den Einzelerläuterungen zum jeweiligen Artikel der DS-GVO ist eine allgemeine Befassung mit der Regelung vorangestellt.

Dies macht das kompakte Werk zu einem rundum gelungenen und empfehlenswerten Kommentar für den Praktiker.

BDSG/DS-GVO: KOMMENTAR ZU DS-GVO, BDSG UND DEN DATENSCHUTZBESTIMMUNGEN VON TMG UND TKG

Dr. Kai-Uwe Plath (Hrsg)

Dr. Kai-Uwe Plath (Hrsg)
»BDSG/DS-GVO: Kommentar zu DS-GVO, BDSG und den Datenschutzbestimmungen von TMG und TKG«

Verlag Dr. Otto Schmidt

3. Auflage 2018
1.700 Seiten
ISBN 978 3 504 56075 1
159,00 Euro

Das Werk von Dr. Kai-Uwe Plath hat das Zeug, um sich als Standardwerk zu etablieren. Das Werk zeichnet nämlich die Besonderheit aus, dass natürlich die DS-GVO aber auch das BDSG sowie die Datenschutzbestimmungen des Telemediengesetzes und des Telekommunikationsgesetzes bearbeitet werden. Damit erhält der Leser gebündelt in einem Werk die Kommentierung für die typischen Datenschutzbestimmungen im unternehmerischen Alltag.

Die Autoren sind vor allem Praktiker aus der Anwaltschaft. Dies schlägt sich positiv in der praxisnahen und nicht unnötig akademischen Erläuterung der Einzelregelungen nieder. Dies soll nicht dahin verstanden werden, dass der Kommentierung der juristische Tiefgang fehlt, darf aber sehr wohl dahin verstanden werden, dass die Autoren darum wissen, um was es in der Praxis geht.

Das Werk ist rundum gelungen. Gerade wenn es aber darum geht, mit nur einem Werk in der Praxis ein weites Spektrum abzudecken, wird das Werk die erste Wahl sein, da die Kommentierung nicht auf ein Gesetz beschränkt ist.

DATENSCHUTZ IM INTERNET - RECHTS-HANDBUCH ZU DS-GVO UND BDSG

Dr. habil. Silke Jandt / Dr Roland Steidle (Hrsg)

Dr. habil. Silke Jandt / Dr Roland Steidle (Hrsg)

»Datenschutz im Internet - Rechtshandbuch zu DS-GVO und BDSG«

Nomos (Verlag)

1. Auflage 2018
532 Seiten
ISBN 978 3 8487 4856 3
89,00 Euro

Das Rechtshandbuch zur DS-GVO und zum BDSG behandelt deren Regelungen mit Blick auf den Datenschutz im Internet. Dementsprechend enthält das Werk auch keine Erläuterung von Einzelregelungen der DS-GVO und des BDSG, sondern behandelt ausgehend von der jeweiligen Datenverarbeitung im Internet die Anforderungen der DS-GVO und des BDSG.

Ausgehend von der einleitenden Darstellung der technischen und rechtlichen Grundlagen werden zunächst die Begriffsbestimmungen und die Grundlagen der Zulässigkeit der Verarbeitung personenbezogener Daten internetspezifisch dargestellt. Hieran schließt sich die Behandlung Internetspezifischer Datenverarbeitungen (bspw. Webdienste, Cloud Dienste, Suchmaschinen, Webanalyse, Over the Top-Dienste, ...) an. Nach einem Kapitel zum technischen und organisatorischen Datenschutz schließen sich die Rechte der Betroffenen, Rechtsschutz für Betroffene und Sanktionen an.

Der Leser erhält durch die Einführungen eine grundlegende Einarbeitung in die Thematik, wobei die Behandlung internetspezifischer Datenverarbeitungen auch eine thematische Befassung ermöglicht. Das Werk eignet sich neben der Einarbeitung vor allem auch als themenspezifisches Nachschlagewerk.

Das Werk ist für jeden zu empfehlen, der sich in die Thematik Datenschutz im Internet einarbeiten oder sie vertiefen möchte.

Rezensionen von

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

TERMINE DER REGIONALGRUPPEN UND ARBEITSKREISE DES BVD

Die wichtigsten Daten der BvD-Gremien

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

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

▶ www.bvdnet.de/arbeitskreise

Die nächsten Treffen unserer Arbeitskreise und Regionalgruppen:

18.01.2019	RG Karlsruhe	**11.04.2019**	AK Krypto
24.01.2019	RG Mitte	**12./13.04.2019**	AK Externe
30.01.2019	AK Sozial	**12.04.2019**	RG Karlsruhe
12.03.2019	RG Ost	**03.06.2019**	RG Ost
15.03.2019	AK Medizin	**04.06.2019**	AK Medizin
22.03.2019	RG Ulm	**07.06.2019**	AK Externe
10.04.2019	AK Sozial	**28.06.2019**	RG Ulm

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

Termine und Anmeldung finden Sie auf unserer Webseite:

▶ www.bvdnet.de

VERNETZEN SIE SICH MIT UNS:

▶ www.bvdnet.de

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

TWITTER: www.twitter.com/bvd_datenschutz

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

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

BVD-STELLENBÖRSE

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

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

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

Anzeige

BvD e.V.
DATENSCHUTZ GESTALTEN

Überblick

Seminare – 1. Halbjahr 2019

ab 399,-- € zzgl. MwSt. *

Termin	Seminar/ Workshop	Ort
24.01.2019	**BvD-Newcomerforum**	Maritim Nürnberg Referenten: Regina Mühlich, Nikolaus Schrenk
07.02.2019	**Datenschutz-Compliance nach DS-GVO – Workshop**	Novotel Frankfurt City Referenten: Markus Gierschmann, Andreas Sachs
11.03.2019	**Haftungsfragen des Verantwortlichen**	Leonardo Royal Hotel Düsseldorf Referent: Dr. Jens Eckhardt, Konrad Menz
13.03.2019	**Auftragsdatenverarbeitung mit Schwerpunkt auf Art. 26 DS-GVO**	ABION Hotel Spreebogen Referent: Thomas Kahl
14.03.2019	**Beschäftigtendatenschutz – Seminar**	ABION Hotel Spreebogen Referentin: Katja Horlbeck
15.03.2019	**Beschäftigtendatenschutz – Workshop**	ABION Hotel Spreebogen Referentin: Katja Horlbeck
25.03.2019	**Die DS-GVO im Überblick**	Fleming´s Express Hotel Frankfurt Referent: Dr. Jens Eckhardt
26.03.-27.03.2019	**Anforderungen & praktische Umsetzung der DS-GVO - 2-tägiges Seminar**	Fleming´s Express Hotel Frankfurt Referent: Nils Steffen
08.04.2019	**Datenschutz für Betriebsräte & Personalvertretungen**	Novotel Frankfurt City Referent: Dr. Christoph Bausewein

* nur für BvD Mitglieder

Information und Anmeldung unter www.bvdnet.de

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 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

Datenschutz

ALLE PFLICHTEN.
ALLES ERKLÄRT.
ALLES NACH PLAN.

Die ca. 50 Pflichten des EU-Datenschutzes sind machbar. Nutzen Sie hierfür unseren Praxisleitfaden!

www.privazyplan.eu

PRIVAZYPLAN®

Auditierung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH

EIN UNTERNEHMEN VON GDD UND BVD

Datenschutz Zertifizierung:
unabhängig – transparent – standard-basiert

www.dsz-audit.de

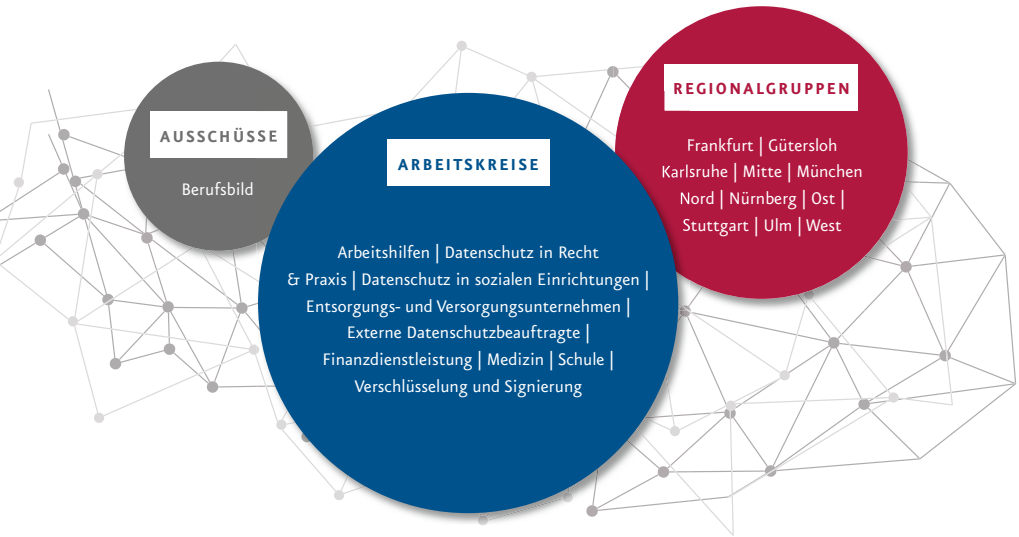
MIT DEM BVD GEMEINSAM DATENSCHUTZ GESTALTEN

BvD e.V.
DATENSCHUTZ GESTALTEN

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert seit über 25 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.

- Seminare und Workshops für einen rechtssicheren Datenschutz im Rahmen der DS-GVO
- Informationen und Begleitung zu Gesetzesvorhaben und Gerichtsentscheidungen
- Unterstützung in der Umstellungsphase der Datenschutz-Grundverordnung
- Austausch auf BvD-Verbandstagen und Fachforen
- Vernetzung bundesweit in Regionalgruppen und Arbeitskreisen
- Materialien für die Datenschutzpraxis in Betrieben und Behörden
- Rabatte bei unseren Verbandspartnern

Für ein Treffen nehmen Sie Kontakt mit dem Sprecher der jeweiligen Regionalgruppen auf der entsprechenden Regionalgruppenseite auf.



BvD-Arbeitskreise

Die BvD-Arbeitskreise setzen sich mit verschiedenen Themen auseinander.

Die Mitarbeit steht allen BvD-Mitgliedern offen.

Derzeit gibt es 9 Arbeitskreise:

- AK Externe Datenschutzbeauftragte
- AK Finanzdienstleistung
- AK Verschlüsselung und Signierung
- AK Medizin
- AK Datenschutz in Recht & Praxis
- AK Schule
- AK Datenschutz in sozialen Einrichtungen
- AK Arbeitshilfen
- AK Arbeitskreis Entsorgungs- und Versorgungsunternehmen (EVU)

BvD-Regionalgruppen

Regionalgruppen ermöglichen den Kontakt der Mitglieder untereinander. Die Gruppen treffen sich regelmäßig zum Austausch.

Auch als Nicht-Mitglied sind Sie gerne unser Gast bei den RGs. Bitte sprechen Sie uns an.

Derzeit gibt es 10 Regionalgruppen:

- In Baden-Württemberg die **Regionalgruppe Karlsruhe**
- in Bayern die **Regionalgruppen München und Nürnberg**
- im Gebiet Großraum Frankfurt die **Regionalgruppen Frankfurt und Mitte**
- im Gebiet Hamburg-Hannover die **Regionalgruppe Nord**
- im Großraum Berlin die **Regionalgruppe Ost**
- im Gebiet um Ulm die **Regionalgruppe Ulm**
- im Gebiet um Stuttgart die **Regionalgruppe Stuttgart**
- im Rhein/Ruhr Gebiet die **Regionalgruppe West**
- in NRW die **Regionalgruppe Gütersloh**

BVD-VERANSTALTUNGEN 2019

Save The Date

05.-06.06.2019

BvD-Verbandstage 2019

Verleihung Datenschutz Medienpreis des BvD (DAME)

am 05. Juni 2019 zur Abendveranstaltung

Ort: ELLINGTON HOTEL BERLIN

23. - 25.10.2019

BvD-Herbstkonferenz zum Datenschutz – WIRTSCHAFT TRIFFT AUFSICHT

Das Bayerische Landesamt für Datenschutzaufsicht, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg und der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. laden zum Informationsaustausch ein.

Ort: im LE MERIDIEN GRAND HOTEL NÜRNBERG

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

Information und Anmeldung unter: https://www.bvdnet.de/termine/verbandsveranstaltung/

Anzeige

Verfügbar als App für iOS und Android oder online im Web-Browser:

Die wichtigsten Tipps und Meinungen zur Datenschutz-Grundverordnung. In der Sonderausgabe der SERVICETODAY.

Exklusiv in der SERVICETODAY App und online: Direkt herunterladen und informieren.

- » Exklusives Interview mit EU-Verhandlungsführer Jan Philipp Albrecht
- » Sabrina Brameshuber von Bitkom Consult zu Custom Audiences
- » Die DSGVO im Service bei SAP-Anwendern
- » Datenschützer Jürgen Hartz im Porträt
- » Datenschutz im Personalbereich: Darauf müssen Recruiter achten
- » Experten von Eversheds Sutherland zur Datenschutzgrundverordnung im Arbeitsverhältnis
- » Serview-Experte Torsten Schneider zum Bundesdatenschutzgesetz
- » Dr. Jens Eckhardt über Bußgelder
- » und vieles mehr

Jetzt im App Store von iOS und Android, bei Amazon und online unter **www.kvd.de**

KVD DER SERVICE-VERBAND

Pliesterbecker Straße 165 | 46284 Dorsten | Tel: 02362 . 9873 - 0 | Fax: 02362 . 9873 - 98 | E-Mail: gs@kvd.de | Internet: www.kvd.de

Anzeige

Datenschutz im Fokus.

ZD – Zeitschrift für Datenschutz
8. Jahrgang 2018. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.
Jahresabonnement € 245,–
Vorzugspreis für BvD-Mitglieder,
für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 185,–.
Vorzugspreis für Studenten und Referendare € 119,–
Abbestellung bis 6 Wochen vor Jahresende.
Preise jeweils inkl. MwSt. zzgl. Vertriebs-/Direktbeorderungsgebühren Inland (€ 13,80/€ 5,–) € 18,80 jährlich.

Mehr Informationen:
www.beck-shop.de/go/ZD

Die große Zeitschrift zum Datenschutz

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

Geschaffen für die Unternehmenspraxis

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

Alles inklusive:

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

3 Hefte gratis

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

Erhältlich im Buchhandel oder bei: **beck-shop.de** | Verlag C.H.BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 158812

C.H.BECK