

BvD-NEWS

Das Fachmagazin für den Datenschutz



Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

Meilenstein für den Datenschutz Das neue Bundesdatenschutzgesetz und die DS-GVO

»DATENSCHUTZ DURCH GESTALTUNG« – der Artikel 25 der DS-GVO – ab S. 8

DAS IT-SICHERHEITSKONZEPT IN DER DS-GVO – ab S. 15

BESCHÄFTIGTENDATENSCHUTZ UNTER DS-GVO & BDSG (NEU) – ab S. 19

EINE DAME FÜR DEN DATENSCHUTZ – ab S. 46

DIE BVD-NEWS WIRD 20 – ab S. 62

DATENSCHUTZ MEDIENPREIS (DAME)

des Berufsverbands der Datenschutzbeauftragten
Deutschlands (BvD) e.V.



DATENSCHUTZ MEDIENPREIS (DAME) DES BVD

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. lobt einen
Filmpreis für Datenschutz aus.

Damit alle in der komplexen digitalen Welt gleiche Chancen auf den Schutz persönlicher Daten haben, muss Datenschutz verständlich erklärt werden. Die Gesetze müssen bei den Bürgern ankommen, Regelungen verständlich und transparent sein. Deshalb lobt der BvD einen Datenschutz Medienpreis aus. Ziel des Preises ist es, das öffentliche Interesse für das Thema Datenschutz rund um zu fördern. Ausgezeichnet werden Beiträge, die Datenschutz verständlich darstellen und zugleich anschaulich erklären.

Bis zum 01. November können sich Filmschaffende, Produktionen, Video-Filmer, Jugendorganisationen, Medienschaffende, Kreative, Verbände und Initiativen mit langen oder kurzen Filmen, mit Spiel- oder Dokumentarfilmen, mit Video-Clips und Animations-Beiträgen um den Preis bewerben.

Eine Jury aus Datenschutzexperten, Medienvertretern und Filmschaffenden wird die eingesandten Beiträge auf fachliche Darstellung, Verständlichkeit, zielgruppengerechte Ansprache und Originalität bewerten.

Mitglieder der Jury sind:

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

Klaus Müller, Vorstand des Verbraucherzentrale Bundesverbands (vzbv)

Frederick Richter, Vorstand Stiftung Datenschutz

Thomas Spaeing, Vorstandsvorsitzender des BvD

Barbara Thiel, Vorsitzende der Datenschutzkonferenz (DSK), Landesbeauftragte für den Datenschutz Niedersachsen

Der Preis ist mit 3.000 Euro dotiert und wird auf dem BvD-Verbandstag 2018 in Berlin übergeben.

Jetzt einreichen!

Einsendeschluss

1. November 2017

INITIATOREN



Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. fördert und vertritt die beruflichen Interessen der Datenschutzbeauftragten in Behörden und Betrieben und setzt sich aktiv für einen rechtskonformen Datenschutz ein.

www.bvdnet.de



Die Initiative „Datenschutz geht zur Schule“ des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. sensibilisiert Schülerinnen und Schüler bundesweit von den 4. Klassen bis zur Berufsschule für den sicheren und bewussten Umgang mit dem Internet und den sozialen Medien.

www.dsgzs.de

KOOPERATIONSPARTNER



klicksafe.de - Die EU-Initiative für mehr Sicherheit im Netz.

In Deutschland ist die Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz gemeinsam mit der Landesanstalt für Medien (LfM) Nordrhein-Westfalen mit der Umsetzung beauftragt.

www.klicksafe.de

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31, 10787 Berlin, Telefon: +49 (0) 30 26 36 77 62, Telefax: +49 (0) 30 26 36 77 63
E-Mail: datenschutzmedienpreis@bvdnet.de, Website: www.bvdnet.de

»DIE DATENSCHUTZ-GERÜCHTEKÜCHE«

»Fake-News« haben Hochkonjunktur – auch beim Datenschutz.



Liebe Leserinnen und Leser,

die Arbeit mit der DS-GVO und dem BDSG-neu ist überall im Gang. Die ersten wertvollen Arbeitshilfen und Arbeitsmaterialien sind auf dem Tisch und viele renommierte Autoren befassen sich mit den neuen Regelungen und ihren Auswirkungen. Darüber hinaus gibt es unzählige Veranstaltungen, die Unternehmen und Datenschützer informieren wollen. Das alles ist erfreulich und hilft uns, die neuen Regelungen im Tagesgeschäft anzuwenden. Allerdings wird mancherorts schlicht Unfug erzählt und da wird es gefährlich. Wenn der Rat vermeintlicher Experten dazu führt, dass sich alle Beteiligten wieder »hinlegen«, dann ist größte Vorsicht geboten.

Zäsur des neuen Datenschutzrechts

Immer wieder berichten Unternehmensvertreter, dass auf Veranstaltungen das neue Recht als »alter Wein in neuen Schläuchen« dargestellt wird. Dies ist genauso falsch wie fahrlässig. Kaum eine Regelung des BDSG-alt hat es unbeschadet in die DS-GVO geschafft und häufig führen bereits kleine Umformulierungen dazu, dass im Ergebnis erhebliche Änderungen erforderlich sind. Die Auslegungen und Praxistipps der Vergangenheit reichen da nicht mehr aus. Das neue europäische Datenschutzrecht macht eine Neubewertung vieler Datenverarbeitungen erforderlich. Ich möchte Ihnen zwei Beispiele dazu geben.

Der Datenschutzbeauftragte ist verantwortlich für den Datenschutz

Sie ahnen es schon: Weder bisher noch in Zukunft war bzw. ist diese Aussage haltbar. Der DSB hat durch die DS-GVO klare Aufgaben, deutlich klarer, als dies bisher der Fall war. Die Verantwortung für den Datenschutz der verarbeitenden Stelle ist ebenfalls sehr klar geregelt: Sie liegt bei der Leitung. Sie kann den DSB bei bestimmten Themen hinzuziehen, der DSB seinerseits muss dann beraten und die Umsetzung prüfen. Er bleibt dabei weisungsfrei und kann weiterhin selbst nichts anweisen. Damit ist er ebenso wenig verantwortlich, wie er auch für die

Verstöße des Verantwortlichen haftet. Solche Aussagen sind zwar immer wieder zu finden, aber sie sind schlicht falsch.

Um die Situation des Datenschutzbeauftragten zu klären, hat der BvD ein Gutachten bei der renommierten Kanzlei Derra, Meyer & Partner in Auftrag gegeben. Dieses Gutachten liegt in Kürze vor und wird dann ausgewertet. Die offizielle Vorstellung erfolgt durch die Gutachter selbst auf der Veranstaltung in Stuttgart am 26. & 27.10.2017. Selbstverständlich werden wir auch in den BvD-News dazu berichten und die Ergebnisse veröffentlichen.

Alles beim Alten auch bei der Technik?

Mit ihren Artikeln in dieser Ausgabe sorgen Marit Hansen (Lfd SH) und Dr. Stefan Brink (LfdI BW) für weitere Klarstellung. So stellt Marit Hansen anschaulich dar, dass die Vorgaben zu Privacy by Design und Privacy by Default eben nicht nur Sache des Anbieters sind sondern auch bei der Entwicklung von Verarbeitungsprozessen und beim Einsatz von Systemen durch den Verantwortlichen berücksichtigt werden müssen. Dr. Stefan Brink räumt mit den Gerüchten zur Videoüberwachung auf (»Alles wie früher...«). Auch wenn im Ergebnis auf die Erfahrungen mit dem § 6b BDSG-alt zurückgegriffen werden kann, so ist die Rechtsgrundlage neu und insbesondere die Pflichten, die sich daraus ergeben, werden uns noch die eine oder andere Nuss zu knacken geben. Von einem »Weiter so!« – kann nicht die Rede sein.

Sie sehen, wir haben also wieder eine ganze Reihe spannender Themen in dieser Ausgabe. Ich wünsche viel Vergnügen bei der Lektüre.

Thomas Spaeing

IMPRESSUM:

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

Herausgeber:

Berufsverband der Datenschutz-
beauftragten 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/
berufsverbandderdatenschutz
beauftragtendeutschlands](http://www.xing.com/companies/berufsverbandderdatenschutzbeauftragtendeutschlands)



[www.twitter.com/bvd_datenschutz](https://www.bvdnet.de/feed/)
<https://www.bvdnet.de/feed/>

Redaktion:

Thomas Spaeing
(V.i.S.d.P., bvd-news@bvdnet.de)
Katrjn Eggert, Rudi Kramer, Jürgen Hartz

Fotos:

123rf.com

Lektorat:

Frank Spaeing

Anzeigen:

Katrjn Eggert
(bvd-gs@bvdnet.de)

Satz und Layout:

Trend Point Marketing GmbH,
Salzuffer 15/16, 10587 Berlin
www.tpmarketing.de

Druck:

Trend Point Marketing GmbH,
Salzuffer 15/16, 10587 Berlin
www.tpmarketing.de

ISSN: 2194-1025

Erscheinungsweise: 3 x jährlich, ca. 2.500 Exemplare
(Mediadaten anfordern unter bvd-gs@bvdnet.de)
Die Redaktion behält sich vor, Beiträge redaktionell
zu überarbeiten und zu kürzen. Namentlich gekenn-
zeichnete Beiträge müssen nicht die Meinung des
BvD e.V. wiedergeben.

EDITORIAL

Editorial: »Die Datenschutz-Gerüchteküche« – *Thomas Spaeing* 3

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Abstimmungserfordernisse nach der DS-GVO – *Thomas Kranig*, Präsident des Bayrischen
Landesamtes für Datenschutzaufsicht 5
»Datenschutz durch Gestaltung«– der Artikel 25 der Datenschutz-Grundverordnung
Marit Hansen, Unabhängiges Landeszentrum für Datenschutz (ULD) 8
Videoüberwachung in der Datenschutzgrundverordnung – *Dr. Stefan Brink*, Landesbeauftragter
für den Datenschutz und die Informationsfreiheit Baden-Württemberg 11
Das IT-Sicherheitskonzept in der DS-GVO – *Dr. Niels Lepperhoff* 15
Beschäftigtendatenschutz unter DS-GVO & BDSG (neu)
Thomas Kahl, Rechtsanwalt, Taylor Wessing 19
Datenschutz-Risikomanagement – *Dipl.-Ök. Stephan Rehfeld* 23
Datenschutz-Grundverordnung – eine sinnvolle Herausforderung oder Provokation für
Kliniken und Krankenhäuser? – *Dr. jur. Siegfried Meyer* 27
DS-GVO weitet Dokumentationspflichten deutlich aus, Datenschutzmanagement
wird zu dynamischem Prozess, der alle Unternehmensbereiche umfasst – *Christian Volkmer* 32

DATENSCHUTZPRAXIS

Was der Datenschutz von der Informationssicherheit lernen kann – vom ISMS zum DSMS
– *Andreas Liefelth*, procion 36
Was steckt hinter der Versiegelten Cloud der Telekom? – *Dr. Hubert Jäger*, CTO Uniscon GmbH 38
Sensibilisierung zum Thema »Soziale Manipulation« – *Stefan Bachmann*, INES IT 42

AUFSICHTSBEHÖRDE

Fragebogen für künftige Unternehmensprüfung nach DS-GVO 44
Erstmals LfDI-Preis für Data Protection and Transparency verliehen 45

GESELLSCHAFT

Eine DAME für den Datenschutz – Der Datenschutz Medienpreis des BvD 46
Wettbewerbsvorteil: Transparente Ansprache – *Sebastian Himstedt* 50

REZENSIONEN

Datenschutz-Compliance nach der DS-GVO – *Kranig, Sachs, Gierschmann* 52
DS-GVO Datenschutz-Grundverordnung VO (EU) – *Gola (Hrsg.)* 53
Datenschutz-Grundverordnung – *Ehmann / Selmayr (Hrsg.)* 54
Datenübermittlung im Konzern – *Matthias Lachenmann* 55
Rechtshandbuch Betrieblicher Datenschutz – *Forgó/Helfrich/Schneider* 56

AUS DEM VERBAND

Weiterhin DS-GVO im Blick - Mitgliederbefragung 2017 – *Dr. Kai-Uwe Loser* 57
»Mit den Jahren wird sie immer jünger.« – Die BvD-News feiert im August ihren 20. Geburtstag
als Mitgliedermagazin 62
Termine der Regionalgruppen und Arbeitskreise des BvD 64
Überblick Seminare und Workshops ab September 2017 65

SERVICE

Wichtige Kontakte im Überblick 66

ABSTIMMUNGSERFORDERNISSE NACH DER DS-GVO

Thomas Kranig,
Präsident des Bayerischen Landesamtes für Datenschutzaufsicht



DS-GVO ist Verordnung und Aufsichtsbehörden sind unabhängig

Die Datenschutz-Grundverordnung ist als Verordnung unmittelbar anwendbar. Das mit einer EU-Verordnung angestrebte Ziel der Harmonisierung des Rechts auf europäischer Ebene kann man nur dann erreichen, wenn alle Beteiligten sich um ein einheitliches Verständnis bemühen. Dies bedeutet zum einen, dass die Verantwortlichen und Auftragsverarbeiter sich einen (momentan noch relativ schwer zu bekommenden) Überblick verschaffen, welche Anforderungen das neue Recht mit sich bringt und sich daran orientieren. Viel wichtiger aber ist, dass die unabhängigen Datenschutzaufsichtsbehörden sich um ein gemeinsames Verständnis bemühen und dieses bei Ausübung ihrer Befugnisse, d.h. bei Beratungen, Kontrollen, Anordnungen und auch Sanktionen zum Ausdruck bringen. Dies kann nur dann funktionieren, wenn alle Aufsichtsbehörden sich bei aller Unabhängigkeit in vielen Fällen zurücknehmen, um ein gemeinsames Ergebnis zu erzielen.

Abstimmungsregelungen in der DS-GVO – Leitlinien

Die Datenschutz-Grundverordnung versucht diesen »systemimmanenten Widerspruch« zwischen einheitlichem Vollzug und Unabhängigkeit der Aufsichtsbehörden in Kapitel VII in insgesamt 17 Artikeln (von insgesamt 99 Artikeln) zu regeln. Dieser Anteil an Vorschriften bringt schon zum Ausdruck, welche Bedeutung der europäische Gesetzgeber einer funktionierenden Zusammenarbeit der Datenschutzaufsicht in Europa beimisst. Wenn man ferner in der DS-GVO nach dem Begriff »Kohärenz«, das heißt-Verfahren zur Gewährleistung einer einheitlichen Rechtsanwendung (so ErwGr. 135) sucht, findet man ihn 32 mal, was auch eine Aussage ist.

Das wirksamste Organ für das einheitliche Verständnis und den einheitlichen Vollzug ist der Europäische Datenschutzausschuss (Ausschuss – Art. 68), in dem alle Mitgliedstaaten der EU durch ihre Datenschutzaufsichtsbehörden bzw. im Fall von mehreren Behörden in einem Mitgliedstaat durch

einen Vertreter repräsentiert sind. Dieser Ausschuss hat zumindest im derzeitigen Verfahrensstand die Hauptaufgabe, Leitlinien zur Konkretisierung der Vorschriften der DS-GVO zu verabschieden, an denen sich die Verantwortlichen und auch die Datenschutzaufsichtsbehörden orientieren können. Dieses Ziel hat sich derzeit schon die Vorläuferorganisation des Ausschusses, die Art. 29-Datenschutzgruppe auf die Fahnen geschrieben und mehrere Working Papers zur DS-GVO veröffentlicht (z. Zt. drei) oder in Planung bzw. schon in der Pipeline (z. Zt. zwölf), die nach Konstituierung des Ausschusses und dem Wirksamwerden der DS-GVO nach dem 25. Mai 2018 als »formelle« Leitlinien veröffentlicht werden sollen. Der Arbeitsaufwand und die Schwierigkeiten, die mit der Erstellung dieser Papiere verbunden sind, sind für Außenstehende kaum vorstellbar. Nachdem die Aufsichtsbehörden davon ausgehen, dass diese Leitlinien in Zukunft deutlich relevanter sein werden als die zahlreichen Working Papers, die die Art. 29-Gruppe bisher veröffentlicht hat, ist verständlich, dass auch die Diskussionen intensiver werden.

Zusammenarbeit (Art. 60 ff.)

In zahlreichen Vorschriften werden die Aufsichtsbehörden zur Zusammenarbeit verpflichtet. Dies betrifft, vereinfacht ausgedrückt, die Fällen mit grenzüberschreitender Bedeutung, die immer dann gegeben ist, wenn Verantwortliche ihre Waren oder Dienstleistungen grenzüberschreitend anbieten. Sofern eine (federführende) Aufsichtsbehörde beabsichtigt, in diesen Fällen hoheitlich tätig zu werden, muss sie den anderen Aufsichtsbehörden Gelegenheit zur Stellungnahme geben und, sofern die anderen Aufsichtsbehörden mehrheitlich zu einem anderen Ergebnis kommen, sich an dem Mehrheitsbeschluss orientieren.

Kohärenzverfahren (Art. 63 ff.)

Soweit die Zusammenarbeit der Aufsichtsbehörden u. a. die Liste für notwendige Datenschutz-Folgenabschätzungen, Verhaltensregeln, Zertifizierungen Standarddatenschutzklauseln betrifft, sieht die DS-GVO ein Kohärenzverfahren (Art. 63) vor. Auch in diesem Verfahren geht der Anstoß von einer (zuständigen) Aufsichtsbehörde aus, die einen Beschlussvorschlag macht, zu dem der Ausschuss dann eine Stellungnahme abgibt.

Von besonderer Bedeutung ist in diesem Verfahren, bei dem es, wie oben ausgeführt, um sehr grundsätzliche und weit reichende Sachverhalte geht, dass hier nicht nur die Aufsichtsbehörden sondern auch die Kommission zum einen die Möglichkeit hat zu beantragen, dass Angelegenheiten, die nach ihrer Auffassung eine allgemeine Geltung beanspruchen oder Auswirkungen auf mehr als einen Mitgliedsstaat haben, vom Ausschuss geprüft werden. Infolge Verfahren hat dann neben den Aufsichtsbehörden wiederum auch die Kommission die Möglichkeit ihre Erkenntnisse zum Sachverhalt, zum Beschlussentwurf oder zu den Standpunkten anderer Betroffener Aufsichtsbehörden einzubringen. Man kann möglicherweise darüber streiten, ob es richtig ist dass die Kommission diese Rolle im Kohärenzverfahren ausüben darf. Man sollte aber nicht darüber streiten, weil die Grundverordnung verabschiedet ist und damit eine für längere Zeit gültige Rechtsnorm. Man kann die Regelung aber auch als Chance sehen, dass die Kommission, die dann bei Abstimmungen nicht stimmberechtigt ist, in den Beratungen ihre Auffassung einbringen kann, um auch transparent zu machen, wo sie von Grenzüberschreitungen im Sinne einer Vertragsverletzung ausgeht, die sie andernfalls im Rahmen eines Vertragsverletzungsverfahrens vor dem Europäischen Gerichtshof geltend machen müsste.

Festzuhalten ist in diesem Zusammenhang auch, dass es nur sehr wenige Entscheidungen gibt, in denen der Ausschuss nach der DS-GVO einen verbindlichen Beschluss trifft (Art. 65). Dies betrifft u. a. die Fälle, dass eine federführende Aufsichtsbehörde einen Einspruch einer anderen Aufsichtsbehörde als nicht maßgeblich oder nicht begründet ablehnt, wenn umstritten ist, welche Aufsichtsbehörde für eine Hauptniederlassung zuständig ist oder wenn eine zuständige Aufsichtsbehörde ein notwendiges Kohärenzverfahren nicht einleitet.

»Mini-Kohärenzverfahren« in Deutschland

Die DS-GVO schreibt den Mitgliedstaaten nicht vor, wie sie die Struktur der Datenschutzaufsichtsbehörden regeln, d.h. ob sie eine oder mehrere Aufsichtsbehörden vorsehen. Wenn es aber mehrere Aufsichtsbehörden in einem Mitgliedstaat (wie z. B. Deutschland) gibt, dann muss der Mitgliedstaat ein Verfahren einführen, mit dem sichergestellt wird, dass die anderen Behörden die Regeln

Pflicht-Update für Datenschutz- beauftragte.

für das Kohärenzverfahren nach Art. 63 einhalten. Um dem Rechnung zu tragen, hat der deutsche Gesetzgeber im neuen Bundesdatenschutzgesetz in den §§ 17 ff. BDSG-neu vorgesehen, dass die Bundesbeauftragte für den Datenschutz und Informationsfreiheit die gemeinsame Vertreterin im Ausschuss für Deutschland ist und ihr als Stellvertreter die Leitung einer Aufsichtsbehörde, die vom Bundesrat bestimmt wird, an die Seite gestellt wird. Davon getrennt ist zu betrachten, was die deutsche Vertretung im Ausschuss sagen kann. Ebenfalls vereinfacht ausgedrückt ist im BDSG-neu geregelt, dass dann, wenn keine einvernehmliche Regelung über einen deutschen Standpunkt zustande kommt, die Aufsichtsbehörden aller 16 Bundesländer und des Bundes, also insgesamt 17, mit Mehrheit beschließen (wobei der Bund auch nur eine Stimme hat), welche Position Deutschland in Europa vertritt.

Ausblick

Sowohl die Regeln der DS-GVO als auch die des BDSG-neu bieten die Möglichkeit die Zusammenarbeit der Aufsichtsbehörden und die Abstimmung im Interesse eines einheitlichen Vollzugs des Datenschutzrechts auf eine gute Basis zu stellen. Regelungen für den Konfliktfall bzw. einen Verstoß gegen die Zusammenarbeitsvorschriften verbunden mit Zwangsmitteln zur Durchsetzung gibt es nicht. Es ist und bleibt deshalb sehr entscheidend, wie die mit ihrer Unabhängigkeit ausgestatteten Aufsichtsbehörden in der täglichen Arbeit bereit sind, Kompromisse zu schließen und Mehrheitsentscheidungen nicht nur zu erdulden, sondern im Zweifel auch gegen die eigene Überzeugung umsetzen. Letztendlich wird zwar der Europäische Gerichtshof verbindlich festlegen, was die DS-GVO uns sagen will. Es ist aber davon auszugehen, dass für diese Gerichtsentscheidungen die Abstimmungsergebnisse der Datenschutzaufsichtsbehörden auf europäischer Ebene durchaus auch ihre Beachtung finden werden.

Über den Autor

Thomas Kranig

Präsident des Bayerischen Landesamtes für
Datenschutzaufsicht



► www.lida.bayern.de



Von Jochen Schneider
2017. 323 Seiten. Kartoniert € 24,90
ISBN 978-3-406-70213-6

Mehr Informationen: beck-shop.de/blgsg

Auch wenn die Datenschutz-Grundverordnung erst 2018 in Kraft tritt, müssen die betrieblichen Datenschutz-Konzepte frühzeitig an die neuen Regelungen angepasst und umgestellt werden.

Der kompakte Band gibt einen **schnellen Überblick** über die neuen Vorgaben und **klärt, was konkret zu tun ist.**

Topaktuell: Mit der deutschen Umsetzungsgesetzgebung, insbesondere zur Stellung des Datenschutzbeauftragten und zum Schutz von Arbeitnehmerdaten.

Anschaulich mit vielen hervorgehobenen **Hinweisen, Tipps, und Mustern.**

Erhältlich im Buchhandel oder bei: beck-shop.de
Verlag C.H.BECK oHG · 80791 München
kundenservice@beck.de | Preise inkl. MwSt. | 167401

2. Datenschutz »by Design«

Die Bezeichnung in der deutschen Sprachfassung »Datenschutz durch Technikgestaltung« ist irreführend, denn in den anderen Sprachen der DS-GVO einschließlich der englischen Verhandlungsfassung tritt das Wort »**Technikgestaltung**« überhaupt nicht in Erscheinung. Richtiger wäre »Datenschutz durch Gestaltung« – ohne eine (vermeintliche) Beschränkung auf »Technik« – gewesen. Auch wenn die Regelung an die Debatten um »Datenschutz durch Technik« seit Mitte der 1990er Jahre anknüpft, würde es zumeist nicht ausreichen, wenn man lediglich einen Blick auf die eingesetzte Technik nähme und die vorhandenen Prozesse und organisatorische und rechtliche Maßnahmen vernachlässigte.

Verpflichtet ist der Verantwortliche: Er muss frühzeitig – bereits bei der Festlegung der Mittel einer Datenverarbeitung – geeignete technische und organisatorische Maßnahmen treffen, um die Anforderungen der DS-GVO umzusetzen. Die Formulierung ähnelt Artikel 32 DS-GVO (»Sicherheit der Verarbeitung«): Der Verantwortliche trifft diese Maßnahmen nämlich »unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen«. Mit dieser Wortwahl werden mehrere Kriterien benannt, die jeweils interpretationsbedürftig sind. Insbesondere der »Stand der Technik« – eigentlich nichts Neues, weil er schon in Artikel 17 der Datenschutz-Richtlinie 95/46/EG erwähnt wurde – hängt stark davon ab, wie der Reifegrad einer Lösung beurteilt wird. Sicherlich sind viele – teilweise jahrzehntealte – Ideen in der wissenschaftlich geprägten Community zu »Privacy & Data Protection Engineering« noch nicht auf dem Markt zu finden. Doch zahlreiche Lösungen haben ihre Praxistauglichkeit schon in Projektdemonstratoren oder lauffähigen Prototypen unter Beweis gestellt. Mit dem Artikel 25 DS-GVO im Rücken ist mit einem Schub der Forschungsergebnisse in Richtung »Stand der Technik« zu rechnen. Es steht zu vermuten, dass sich einerseits Firmen in diesem Bereich spezialisieren, andererseits auch geeignete Software-Komponenten zunehmend auf Open-Source-Plattformen zu finden sein werden.

Die Verantwortlichen, die die Regelungen umsetzen möchten, können dies zumeist nur tun, soweit die von ihnen ausgewählten Produkte, Dienstleistungen und Anwendungen diese Eigenschaften mitbringen. Die DS-GVO richtet sich zwar nicht direkt an die Hersteller, aber fordert in Erwägungsgrund 78, dass diese »ermutigt« werden sollen, Datenschutz durch Technikgestaltung und durch da-

tenschutzfreundliche Voreinstellungen in ihren Produkten, Dienstleistungen und Anwendungen zu berücksichtigen und es dadurch den Verantwortlichen zu ermöglichen, ihren datenschutzrechtlichen Verpflichtungen nachzukommen. Auf der einen Seite ist dies ein Aufruf an Fördergeber, auf der anderen Seite verweist Erwägungsgrund 78 auf öffentliche Ausschreibungen, die die Anforderungen des Artikels 25 DS-GVO herausstellen sollen und die Vorbildfunktion des öffentlichen Sektors betonen. Eine wichtige Rolle werden außerdem Dienstleister im Rahmen einer Auftragsverarbeitung gem. Artikel 28 DS-GVO spielen.

Die Verantwortlichen werden den »Stand der Technik« stets in den Blick nehmen müssen, weil dieser nicht nur die noch nicht ausgereiften Maßnahmen ausfiltert, sondern auch Leitplanken für das erwartete Mindestmaß definiert. Die Aufsichtsbehörden sollten auf europäischer Ebene hierzu klare Empfehlungen erarbeiten. Vorteilhaft wäre ein gut gepflegtes Repository über die Maßnahmen, die in typischen Situationen als Stand der Technik erwartet werden. Hier muss jedoch bei den Datenschutz-Lösungen genau hingeschaut werden: Die effektive Wirksamkeit von Anonymisierungstechniken beispielsweise hängt üblicherweise von dem jeweiligen Kontext und den verarbeiteten Daten ab – »one size fits all« funktioniert oft nicht. Es wird also nicht ausreichen, sich die »richtigen« Privacy-Enhancing Technologies zusammenzuklicken, um das gewünschte Ergebnis zu erreichen.

3. Datenschutz »by Default«

Jede deutschsprachige Kommentierung des Artikel 25 Abs.2 DS-GVO sollte mit einer Warnung beginnen. Leider hat sich nämlich ein Fehler in die deutsche Sprachfassung eingeschlichen, der sich in anderen Versionen einschließlich des englischen Texts nicht findet. Es wurde ein »grundsätzlich«, also eine Formulierung für Ausnahmen, hineingemogelt:

»Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung **grundsätzlich** nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.«

(Artikel 25 Abs.2 Satz 1 DS-GVO – deutsche Fassung;
Hervorhebung und Streichung durch die Verfasserin)

Im Vergleich dazu lautet die englische Sprachfassung:

»The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.«

(Artikel 25 Abs.2 Satz 1 DS-GVO – englische Fassung) ▶

Die Regelung des Artikels 25 Abs.2 DS-GVO ist sehr mächtig: Die typischen relativierenden Bedingungen der DS-GVO, beispielsweise im Artikel 25 Abs.1 oder Artikel 32 DS-GVO, fehlen in dieser Vorschrift. Es ergibt sich also eine Verpflichtung für den Verantwortlichen, dass bei einer Verarbeitung gemäß den Voreinstellungen keine überschießenden personenbezogenen Daten (die für den jeweiligen Verarbeitungszweck nicht erforderlich sind) verarbeitet werden. Eigentlich eine Selbstverständlichkeit – und auch schon in Artikel 5 Abs.1 Buchst. b und c mit den Grundsätzen der Zweckbindung und der Datenminimierung zum Ausdruck gebracht, aber keinesfalls gelebte Praxis.¹

Dennoch hat diese Betonung des Prinzips »Datenschutz durch datenschutzfreundliche Voreinstellungen« besondere Relevanz. Software-Entwickler lernen, dass sie gemäß dem »Principle of least astonishment« (Prinzip der geringsten Verwunderung) ihre Voreinstellungen bestimmen sollen und dass ein Großteil der Nutzenden dann auch keine Umkonfiguration vornimmt. Die Idee des »Datenschutzes by Default«: Erst wenn Nutzende bewusst sich dafür entscheiden, mehr personenbezogene Daten herauszugeben oder eine umfangreichere Verarbeitung zuzulassen, soll dies möglich sein, aber nicht in der initialen Konfiguration beim Anfang der Nutzung. Damit können sich die Nutzenden zunächst in einer datensparsameren Variante mit dem System vertraut machen, bevor sie informiert, bewusst und freiwillig möglicherweise zusätzliche Datenfreigaben erteilen.

Überträgt man »Datenschutz by Default« auf die heutige Internet-Welt, muss sich eine Menge ändern: Da Tracking und zielgerichtete Werbung nicht zum originären Zweck der Dienstenutzung gehören, dürfte dafür ohne aktives Zutun der Nutzenden keine Datenverarbeitung stattfinden. Sofern eine nutzerbezogene Personalisierung für die Verarbeitung nicht erforderlich ist – beispielsweise beim Online-Shopping – würden die dafür üblicherweise verwendeten Daten in der Initialkonfiguration nicht zur Verfügung stehen, sondern die Nutzenden müssten dies explizit freigeben.

¹ Leon u. a.: Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising, in: Proc. CHI '12, S. 589-598, 2012.

Artikel 25 Abs.2 Satz 3 DS-GVO definiert genauer, wie das Erforderlichkeitsprinzip in diesem Zusammenhang zu verstehen ist. Dies umfasst die gesamte Verarbeitung einschließlich frühestmöglicher Löschung und maximal restriktiver »Accessibility« (»Zugänglichkeit«) der Daten, was u. a. Anforderungen an Speicherorte und Zugriffsmöglichkeiten stellt.

Artikel 25 Abs.3 DSGVO konkretisiert die Situation, dass »personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden« darf, beispielsweise beim Hochladen von Daten in ein Soziales Netzwerk, in dem man nur seine Freunde und nicht potenziell die gesamte Internet-Öffentlichkeit informieren möchte.

4. Fazit

Artikel 25 DS-GVO gehört zu denjenigen Vorschriften, deren Potenzial sich über die Zeit entfalten kann, wenn die heutige Ausnahmesituation eines eingebauten Datenschutzes (hoffentlich) zur Regel wird. Schon heute sei den Verantwortlichen dringend angeraten, die Maßnahmen, die in Erwägungsgrund 78 erwähnt werden, für ihre Datenverarbeitung zu prüfen. Unabdingbar ist das Vorhalten schriftlich niedergelegter interner Strategien (englisch: »adopt internal policies«) zur Umsetzung des Artikels 25 DS-GVO.

Über die Autorin



Marit Hansen

Landesbeauftragte für Datenschutz
Schleswig-Holstein
Diplom-Informatikerin

► www.datenschutzzentrum.de



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

VIDEOÜBERWACHUNG IN DER DATENSCHUTZGRUNDVERORDNUNG

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

Videoüberwachung ist das »Brot und Butter-Thema« der Datenschützer. Umso problematischer, dass mit der DS-GVO eine Regelung ab Mai 2018 wirksam wird, die den altbekannten § 6b BDSG ablöst, aber für diese Materie keine spezifische Neuregelung anbietet. Die Datenschützer stehen daher gleich vor zwei Aufgaben: sich vom alten BDSG zu lösen und aus den allgemeinen Vorschriften der DS-GVO die einschlägigen Bestimmungen für die Thematik Videoüberwachung herauszufiltern. Keine ganz leichten Aufgaben ...



1. Es kann nur einen geben: DS-GVO

Der Einschnitt, der uns mit dem 25. Mai 2018 bevorsteht, ist ein radikaler: Die DS-GVO löst in ihrem Geltungsbereich alle nationalen Datenschutzbestimmungen ab. Dieser Umbruch ist nicht nur für die nationalen Gesetzgeber schwer zu verdauen – auf die untauglichen Versuche des Bundesgesetzgebers, ohne erkennbare Rechtsgrundlage im BDSG neu an vielen Stellen nationale Sonderwege zu beschreiben (vgl. insbesondere § 4 BDSG neu), soll hier erst gar nicht eingegangen werden, sondern auch für die

Rechtsanwender. Sie hatten sich an die nationalen Datenschutzvorschriften, hier § 6b BDSG, so gewöhnt, dass die Versuchung, das angesammelte Wissen nun einfach der DS-GVO unterzuschieben, groß sind. Zumal diese Verordnung ja noch nicht einmal spezifische Bestimmungen zum Thema Videoüberwachung enthält. Dennoch sei auch an dieser Stelle mit aller Klarheit gesagt: Wer versucht, einzelne Regelungselemente oder Anwendungsprinzipien des § 6b BDSG, etwa zum berechtigten Interesse oder zur Löschung der DS-GVO »unterzujubeln«, der begeht einen un-

verzeihlichen Fehler. Die DS-GVO ist eine neue, selbstständige, aus sich selbst heraus und mit dem Methoden des europäischen Rechts auszu- legende Rechtsmaterie. »Berechtigtes Interesse« nach Art. 6 Abs. 1 lit. f DS-GVO ist keineswegs identisch mit dem »berechtigten Interesse« des § 6b Abs. 1 Nr. 3 BDSG. Es ist nicht ausgeschlos- sen, dass die Auslegung beider Tatbestandsmerk- male zum gleichen Ergebnis führt, aber eben auch nicht sicher. Wir alle werden uns nach dem 25. Mai 2018 auf die neue Rechtsmaterie einlas- sen müssen – und uns vor »false friends« und Ar- gumentationen à la »kennen wir schon, ist genau dasselbe« hüten müssen.

2. Welche Regelungen der DS-GVO sind für die Videoüberwachung einschlägig?

Mangels spezifischer Rechtsgrundlage ist für die Prüfung der Rechtmäßigkeit der Datenverarbei- tung durch Videokameras und -anlagen zunächst auf die Generalklausel in Artikel 6 Absatz 1 lit. f DS-GVO abzustellen.

- a) Danach ist die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grund- freiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind han- delt.
- b) Vergleichbar mit § 1 Abs. 2 Nr. 3 a.E. BDSG gewährt Artikel 2 Absatz 2 lit. c DS-GVO aller- dings ein sogenanntes »Haushaltsprivileg«. Die Verordnung findet also keine Anwendung auf die Verarbeitung personenbezogener Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tä- tigkeiten und somit ohne Bezug zu einer be- ruflichen oder wirtschaftlichen Tätigkeit vor- genommen wird (vgl. dazu den einschlägigen Erwägungsgrund 18).
- c) Soll die Berechtigung einer Videoüberwachung auf eine Einwilligung im Sinne des Artikel 7 DS-GVO gestützt werden, dürften die Vor- aussetzungen dieser Vorschrift allerdings nur in seltenen Einzelfällen erfüllt sein. Zunächst einmal gilt für die Einwilligung in die Video-

überwachung das, was für jede Einwilligung in Datenverarbeitungen gilt: Sie ist unpraktisch, weil die Erhebung mühevoll ist; sie ist unzu- verlässig, weil die Einwilligung jederzeit ohne Angabe von Gründen und ohne Erfordernis eines berechtigten Interesses widerrufen wer- den kann; und sie ist fehleranfällig, weil eine vollständig informierte Einwilligung eine sehr umfassende Aufklärung voraussetzt.

Wichtig ist auch zu wissen: Alleine das Be- treten eines gekennzeichneten Erfassungsbe- reichs von Videokameras kann nicht als »ein- deutig bestätigende Handlung« und erst recht nicht als informierte Einwilligung i. S. d. Artikel 4 Nr. 11 DS-GVO gewertet werden.

- d) Die nach Artikel 6 Absatz 1 lit. f durchzufüh- rende Prüfung folgt im Wesentlichen den be- reits aus dem BDSG bekannten Kriterien, also der Wahrung berechtigter Interessen nach Maßgabe einer Erforderlichkeitsprüfung unter Abwägung mit gegenläufigen Interessen. Hin- sichtlich des Tatbestandsmerkmals des »be- berechtigten Interesses« kann die bisherige Ka- suistik eine Orientierung geben – aber eben nicht blindlings übernommen werden (vgl. oben 1). Neu ist aus deutscher Sicht in jedem Falle die Berücksichtigung des sog. »Drittinter- esses«. Als »Dritter« kommen gemäß Artikel 4 Nr. 10 DS-GVO sowohl private als auch juris- tische Personen in Betracht. Typische »Dritte« wären demnach etwa Mieter oder beispie- lweise Versicherer.

Im Rahmen der Erforderlichkeitsprüfung ist nach wie vor zu fragen, ob alternative Maß- nahmen, die nicht oder weniger tief in das Recht auf Schutz personenbezogener Daten eingreifen, im konkreten Einzelfall in Betracht kommen. Bei der anschließenden Interessen- abwägung ergibt sich aus Erwägungsgrund 47 allerdings eine Relativierung des bisher strikt objektiven Ansatzes, da Maßstab nunmehr die »vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Ver- antwortlichen« beruhen, zu berücksichtigen sind. Damit ist neben den subjektiven Erwar- tungen des Betroffenen auch entscheidend, was ein objektiver Dritter vernünftiger Weise erwarten kann und darf. Entscheidend wird daher auch sein, ob die Videoüberwachung in bestimmten Bereichen der Sozialsphäre ty-

pischerweise akzeptiert oder abgelehnt wird. Die Prüfung wird damit deutlich vielschichtiger – und ihr Ergebnis weniger vorhersagbar. Änderungen ergeben sich auch im Hinblick auf die Prüfungstiefe: Anders als das BDSG, das lediglich eine summarische Prüfung fordert, verlangt die DS-GVO eine tatsächliche Interessenabwägung im konkreten Einzelfall sowohl im Hinblick auf die Interessen der Verantwortlichen als auch der Betroffenen. Ein Abstellen auf abstrakte oder auf vergleichbare Fälle genügt den Anforderungen der DS-GVO im Hinblick auf die Prüfungstiefe gerade nicht (mehr).

- e) Neben der Rechtmäßigkeit der Verarbeitung fordert die DS-GVO in Artikel 5 Absatz 1 lit. a ferner, dass die personenbezogenen Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Mit dieser Regelung sowie den sich aus Artikel 12 ff. DS-GVO ergebenden Anforderungen sind die Transparenzpflichten in jedem Fall stark angestiegen. Insbesondere die Informationspflichten nach Artikel 13 Absatz 1 und 2 DS-GVO umfassen als Mindestanforderungen:
- Umstand der Beobachtung – Piktogramm, Kamerasymbol.
 - Identität des für die Videoüberwachung Verantwortlichen – Name einschl. Kontaktdaten (Artikel 13 Absatz 1 lit. a DS-GVO).
 - Kontaktdaten des betrieblichen Datenschutzbeauftragten – soweit bestellt, dann aber zwingend (Artikel 13 Absatz 1 lit. b DS-GVO).
 - Verarbeitungszwecke und Rechtsgrundlage in Schlagworten (Artikel 13 Absatz 1 lit. c DS-GVO).
 - Angabe des berechtigten Interesses – soweit die Verarbeitung auf Artikel 6 Abs.1 lit. f DS-GVO beruht (Artikel 13 Absatz 1 lit. d DS-GVO).
 - Dauer der Speicherung (Artikel 13 Absatz 2 lit. a DS-GVO).
 - Hinweis auf Zugang zu den weiteren Pflichtinformationen gem. Artikel 13 Absatz 1 und 2 DS-GVO (wie Auskunftsrecht, Beschwerderecht, ggf. Empfänger der Daten).
- f) Dies hat erhebliche Konsequenzen: Eine intransparente Videoüberwachung steht nicht im Einklang mit der DS-GVO (Artikel 5, 13

DS-GVO) – und das stellt einen Bußgeldtatbestand nach Artikel 83 Abs.5 DS-GVO dar. Nach dieser Vorschrift werden Verstöße mit Geldbußen von bis zu 20 Mio. Euro bzw. einer Strafe von bis zu 4% des weltweit erzielten Gesamtjahresumsatzes des Verantwortlichen belegt – eine wirklich exorbitante Drohung. Die Aufsichtsbehörde kann darüber hinaus gem. Artikel 58 Abs.2 lit. d DS-GVO eine Anweisung aussprechen.

- g) Die Daten der Videoüberwachung sind unverzüglich zu löschen, wenn sie zur Erreichung der Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Artikel 17 Absatz 1 lit. a DS-GVO) oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen. Ob eine Sicherung des Materials notwendig ist, dürfte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können. Unter Berücksichtigung von Artikel 5 Absatz 1 lit. c und e DS-GVO – »Datenminimierung« und »Speicherbegrenzung« – sollte demnach grundsätzlich, wie bisher auch Vorgabe der deutschen Aufsichtsbehörden, nach 48 Stunden eine Löschung erfolgen.
- h) Die digitale Videoüberwachung in Echtzeit (direkte Übertragung der Bilddaten auf einen Monitor ohne Speicherung der erhobenen Daten – Kamera-Monitor-Prinzip) stellt ebenfalls eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten nach der DS-GVO dar und ist daher nach den genannten Vorschriften zu beurteilen.
- i) Weitere formelle Vorgaben der DS-GVO sind zu beachten: In dem nach Artikel 30 Absatz 1 DS-GVO zu erstellenden Verzeichnis sind die einzelnen Videokameras auszuweisen und u.a. zu dokumentieren, welchem Zweck die Verarbeitung dient, warum sie notwendig ist, welche Risiken für die Rechte und Freiheiten der betroffenen Person bestehen und welche Abhilfemaßnahmen erwo-gen bzw. getroffen wurden.

Ferner ist gemäß Artikel 35 Absatz 3 lit. c DS-GVO bei einer systematischen umfangreichen (Erwägungsgrund 91: weiträumigen) Überwachung öffentlich zugänglicher Bereiche eine Datenschutz-Folgenabschät-

zung nach Absatz 1 dieser Norm erforderlich. In derartigen Fällen hat vor dem Einsatz der Videoüberwachung eine Bewertung der spezifischen Eintrittswahrscheinlichkeit und der Schwere des Risikos für die Datenschutzrechte Betroffener unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Ursachen des Risikos zu erfolgen. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen der Verordnung nachgewiesen werden soll (vgl. Erwägungsgrund 90).

Ob eine Datenschutz-Folgenabschätzung auch für die systematische Überwachung nicht öffentlich zugänglicher Bereiche erforderlich ist, wird derzeit von den Aufsichtsbehörden geprüft. Eine hohe Eintrittswahrscheinlichkeit und die Schwere des Risikos in spezifischen Fällen sprechen dafür, Videoüberwachungen jedenfalls in Bereichen der Privatsphäre einer Datenschutz-Folgenabschätzung zu unterziehen.

3. Fazit

Auch wenn die DS-GVO also keine expliziten Vorgaben für die Videoüberwachung macht und sie – bis auf Erwägungsgrund 91 – noch nicht einmal als Datenverarbeitungsform erwähnt: Die formellen und materiellen Anforderungen für den Einsatz einer Videoüberwachung werden mit Inkrafttreten der DS-GVO im Vergleich zum BDSG keineswegs abgesenkt werden. Sie bleiben vielmehr hoch und nach wie vor sehr komplex. Daher sollten sich Betreiber von Videoüberwachungsanlagen schon zum frühen Zeitpunkt intensiv mit der neuen Rechtslage auseinandersetzen und prüfen, ob die aktuell betriebene Videoüberwachungsanlage auch den künftig geänderten Anforderungen entspricht. Die Aufsichtsbehörden werden schon in Kürze ihre Vorstellungen über die einschlägigen Anforderungen im Rahmen von »Kurzpapieren« veröffentlichen; an diese Orientierungshilfe lehnt sich dieser Beitrag bereits an.



Über den Autor

Dr. Stefan Brink

Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg

► www.baden-wuerttemberg.datenschutz.de



Anzeige

- Externe Datenschutzbeauftragte -

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

Berufs-Haftpflichtversicherung für 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 eDSB zugeschnitten)
- Tätigkeit ‚Auditor für Datenschutz‘ beitragsfrei eingeschlossen
- niedrige Einsteigerprämie sowie professionelle Beratung

NEU: - inkl. EU-DSGVO
- hohe Deckungssummen
zu verbesserten Konditionen

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





DAS IT-SICHERHEITSKONZEPT IN DER DS-GVO

Dr. Niels Lepperhoff

1. Einleitung

Der Gesetzgeber hat mit der Datenschutz-Grundverordnung (DS-GVO) eine längst fällige Aktualisierung seines Sicherheitsverständnisses vorgenommen. § 9 BDSG und seine Anlage stellen einzelne Maßnahmen in das Zentrum der Betrachtung. Legendär sind Listen von Sicherheitsmaßnahmen, die die acht in § 9 Anlage BDSG definierten Kategorien (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot) füllen. Diese Listen muten nicht selten willkürlich an (»Türschloss, Virenschanner, Backup, Firewall ...«). Ihr wichtigster Nachteil liegt jedoch in der fehlenden Nachvollziehbarkeit: Warum wurden diese Maßnahmen getroffen? Gegen welche Gefahren sollen sie schützen?

Art. 32 Abs.1 DS-GVO stellt deshalb folgerichtig die Abwägung zwischen den Risiken für die Betroffenen gegenüber den Implementierungs-

kosten in den Mittelpunkt. Damit knüpft die DS-GVO an ein systematisches und nachvollziehbares Verfahren an.

2. IT-Sicherheitskonzept: Anforderungen und Inhalte

Der Implementierung von Sicherheitsmaßnahmen geht nach Art. 32 Abs.1 DS-GVO eine Risikoabwägung voraus. Diese Risikoabwägung unterliegt der Rechenschaftspflicht von Art. 5 Abs.2 DS-GVO, d.h. sie sollte aus Nachweisgründen dokumentiert werden und stellt letztlich ein Sicherheitskonzept dar.¹ Die Inhalte speisen sich einerseits aus weiteren Vorgaben des Art. 32 DS-GVO aber auch aus der Anforderung, den Stand der Technik zu berücksichtigen (Art. 32 Abs.1 S. 1 DS-GVO).

Die Norm EN 45020 Normung - Allgemeine Begriffe (ISO/IEC Guide 2:2004) definiert in Ziffer 1.4 »Stand der Technik« wie folgt: ▶

¹ Lepperhoff, N. (2016): Mehr gesetzliche Pflichten für IT-Verantwortliche. Konsequenzen aus der neuen EU-Datenschutz-Grundverordnung (Teil 1). in: IT-Sicherheit 02/2016, S. 64 – 69.

»Stand der Technik: entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung«

Normen und Standards geben auch den Stand der Technik wieder. Insofern ist es naheliegend und mit Blick auf die Rechenschaftspflicht auch geboten, sich bei der Erstellung des Sicherheitskonzepts ebenfalls an Normen und Standards zu orientieren. Eine Möglichkeit stellt der BSI-Standard 100-2² dar. Dieser ist im Unterschied zu ISO-Normen kostenfrei zugänglich.

Normen und Standards können helfen, das Sicherheitskonzept zu strukturieren und eine geeignete Methode zur Risikobeurteilung zu verwenden. Eine 1:1 Übernahme ist indes regelmäßig nicht möglich, da Art. 32 DS-GVO eine eigene Risikoabwägung vorschreibt. Sie stellt auf die Risiken der Betroffenen ab. Normen und Standards aus der Sicherheit betrachten regelmäßig stattdessen die Risiken für das Unternehmen. Bestehende Sicherheitskonzepte sind deshalb ebenfalls zu überprüfen, ob sie die Vorgaben des Art. 32 DS-GVO erfüllen.

Die DS-GVO verlangt »ein dem Risiko angemessenes Schutzniveau« zu etablieren. Schutzziele sind dabei:

- »Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme auf Dauer sicherzustellen« und
- die »Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen«.
- Für die Auswahl von Maßnahmen sieht Art. 32 Abs.1 DS-GVO vor, abzuwägen zwischen
- den Implementierungskosten auf der einen Seite und
- der Verarbeitungsart,
- dem Verarbeitungsumfang,

- den Umständen und den Zwecken der Verarbeitung sowie
- der Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten der von der Verarbeitung betroffenen Personen (Mitarbeiter, Nutzer, Kunden, Lieferanten usw.) auf der anderen Seite.

Bei der Betrachtung der »Eintrittswahrscheinlichkeit und Schwere des Risikos für die persönlichen Rechte und Freiheiten« sind sowohl die Konsequenzen aus der erwünschten Datenverarbeitung zu berücksichtigen wie auch die Risiken unzulässiger oder unerwünschter Vorkommnisse. Konkret müssen in der Abwägung insbesondere die Risiken folgender ungewollter Ereignisse berücksichtigt werden (Art. 32 Abs.2 DS-GVO):

- Vernichtung,
- Verlust,
- Veränderung,
- unbefugte Weitergabe und
- unbefugter Zugang.

Der Ausdruck »persönliche Rechte und Freiheiten« zielt auf alle Rechte und Freiheiten einer Person ab und weist über das Informationelle Selbstbestimmungsrecht hinaus. Damit erkennt der Gesetzgeber an, dass eine Verarbeitung personenbezogener Daten Auswirkungen bspw. auf die körperliche Unversehrtheit (vernetzte Insulinpumpe, du bist gemeint) aber auch die Meinungsfreiheit haben kann. Die Charta der Grundrechte der Europäischen Union³ kann als Ausgangspunkt dienen, weitere einschlägige Rechte und Freiheiten zu bestimmen.

Die BSI Grundschatzkataloge⁴ kennen hunderte von Gefahren. Sie bieten deshalb einen guten Ausgangspunkt, alle Gefahren zu bestimmen, denen die personenbezogenen Daten der Betroffenen ausgesetzt sind. Alle Gefahren, die für die Betroffenen unter Berücksichtigung der verarbeiteten Daten nicht zu einem Schaden führen können, können gestrichen werden. Anschließend ist zu prüfen, ob zusätzliche Gefahren berücksichtigt werden müssen. Aus den Gefahren lassen sich unter Schätzung der Eintrittswahrscheinlichkeit und Schadensfolgen die Risiken für die Betroffenen bestimmen.

² Mit BSI-Standard 100-2 liegt der Nachfolger als Entwurf vor.

³ 2010/C 83/02, URL: http://www.europarl.europa.eu/germany/resource/static/files/europa_grundrechtcharta/_30.03.2010.pdf

⁴ URL: https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

3. Vorschlag für ein integriertes Konzept

Neben dem Schutz personenbezogener Daten ist ein Unternehmen gut beraten, auch die eigenen Werte zu schützen. Diese sind u.U. anderen Risiken ausgesetzt, d.h. sie sollten gesondert betrachtet werden. Weiterhin schreibt §13 Abs.7 TMG für Telemedien Sicherheitsmaßnahmen vor.

§13 Abs.7 TMG gilt neben der DS-GVO, da er primär auf eine Stärkung der Sicherheit des Dienstes an sich abzielt. Der Schutz personenbezogener Daten ist neben dem Schutz vor unerlaubten Zugriffen und Sicherung gegen Störungen eine dritte Aufgabe.

§13 Abs.7 TMG nennt drei Schutzanforderungen:⁵

- Schutz vor unerlaubtem Zugriff auf die für Telemedienangebote genutzten technischen Einrichtungen (Nr. 1),

- Sicherung gegen Verletzungen des Schutzes personenbezogener Daten (Nr. 2a) und
- Sicherung gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind (Nr. 2b).

Die DS-GVO ergänzt mit Art. 32 §13 Abs.7 TMG um eine Konkretisierung wie der Schutz personenbezogener Daten auszugestalten sei. Insofern muss man sich in der Praxis nur noch mit Nr. 1 und Nr. 2b beschäftigen.

Es bietet sich an, ein kombiniertes Konzept zu erstellen, das sowohl die Risiken für die Unternehmenswerte, Vorgaben aus der DS-GVO sowie die des TMG berücksichtigt (Tabelle 1). Aus allen drei Perspektiven lässt sich ein Schutzbedarf ableiten. Mittels der Maximum-Methode, d.h. des jeweils höchsten ermittelten Schutzbedarfs, wird der Gesamtschutzbedarf bestimmt. Diese dient als Ausgangspunkt, um die notwendigen Maßnahmen zu bestimmen. ▶

	Unternehmenswerte	Systemschutz	Schutz personenbezogener Daten
Gesetz	-/-	§ 13 Abs.7 TMG	Art. 32 DS-GVO
Schutzziele	<ul style="list-style-type: none"> • Vertraulichkeit • Integrität • Verfügbarkeit 	<ul style="list-style-type: none"> • Schutz vor unerlaubtem Zugriff • Sicherung gegen Störungen 	<ul style="list-style-type: none"> • Vertraulichkeit • Integrität • Verfügbarkeit • Belastbarkeit
Gegenstand	Unternehmenswerte	Technisches System	Risiken des Betroffenen
Risiko Methode	z. B. BSI-Grundschutz	z. B. BSI-Grundschutz	Art. 32 DS-GVO
Schranken	Wirtschaftlich sinnvoll	Wirtschaftlich zumutbar	Risikoangemessen
Schutzbedarf	Maximum aus allen Perspektiven		
Maßnahmen	Basierend auf Schutzbedarf		
Wirksamkeitstests	Konzeption der Wirksamkeitstests aller Maßnahmen		

Tabelle 1: Kombiniertes Sicherheitskonzept

⁵ Ausführlich erläutert in Lepperhoff, N.; Papendorf, M. (2016): Bedeutung der jüngsten Änderungen des §13 Abs.7 TMG. In: DuD 2/2016, S. 107-110.

4. Regelmäßige Wirksamkeitstests

Die Wirksamkeit der Maßnahmen muss regelmäßig überprüft werden (Art. 32 Abs.1 lit. d DS-GVO). Aufgrund der Rechenschaftspflicht sollten die Prüfhandlungen und ihr Ergebnis dokumentiert werden. Dazu zählt bspw. die tägliche Kontrolle, ob das Backup erfolgreich durchgeführt worden ist. Um Kosten zu sparen bietet es sich an, bei der Planung der Maßnahmen deren Kontrolle mit zu berücksichtigen.

Wie und in welchen Abständen Tests durchgeführt werden sollen, ist nicht geregelt. Hier kommt der Stand der Technik und die bereits aus dem Sicherheitskonzept bekannte Abwägung zum Tragen. Es sei daran erinnert, dass die Pflicht, Wirksamkeitstest durchzuführen, keine Rechtsgrundlage zur Verarbeitung personenbezogener Daten darstellt. Diese bemisst sich nach den bekannten Vorschriften insbesondere Art. 6 DS-GVO.

5. Nach dem Konzept ist vor dem Konzept

Da sich der Stand der Technik laufend ändert, neue Angriffsmethoden entwickelt werden und durch sich stetig erhöhende Rechenleistung Brute Force Angriffe immer leistungsfähiger werden, verändert sich die Abwägung ebenfalls. Eine periodische Überprüfung und Anpassung ist deshalb zwingend erforderlich (Art. 24 Abs.1 DS-GVO). Es empfiehlt sich einen entsprechenden Aktualisierungsprozess zu implementieren.

6. Erleichterungen für kleine Unternehmen?

Wie ausgeführt stellt Art. 32 Abs.1 DS-GVO die Risiken für die Betroffenen in das Zentrum der Abwägung. Die Unternehmensgröße geht indes nicht mit ein. Das ist sachgerecht, da der Schutz von Grundrechten nicht von der Leistungsfähigkeit des Verarbeitenden abhängen sollte. Die dargestellten Anforderungen gelten deshalb für Ein-Personen-Unternehmen gleichermaßen wie für Konzerne. Um es ganz deutlich zu sagen, ein Unternehmen, das kein Sicherheitskonzept bezahlen kann, ist grundsätzlich auch nicht in der Lage, personenbezogene Daten angemessen zu schützen.

7. Was ist mit IT-Dienstleistern?

Für die Erstellung des Sicherheitskonzepts sieht Art. 32 Abs.1 DS-GVO das Unternehmen und den Auftragsverarbeiter in der Pflicht. Wer seine IT extern betreuen lässt, sollte sich überlegen,

- ob er das Konzept selber erstellt oder
- seinen IT-Dienstleister mit der Erstellung beauftragt.

Ein selber erstelltes Sicherheitskonzept hat den Vorteil, dass der Dienstleister prüfbare Vorgaben erhält. Nachteilig sind die Knowhow-Anforderung und der Ressourcenbedarf. Beides ließe sich auch durch einen externen Spezialisten decken.

Erstellt der IT-Dienstleister das Konzept selber, kann er seine Expertise ausspielen und es auf seine Leistungsfähigkeit zuschneiden. Er formuliert seine Vorgaben selber. Aus Sicht des Unternehmens bedeutet das häufig ein Kontrollverlust, da die Güte des Konzepts mangels Knowhow nicht beurteilt werden kann.

Auf jeden Fall sollte geregelt werden, wer das Sicherheitskonzept erstellt, und wie der IT-Dienstleister einbezogen wird. Das gilt auch für die Aktualisierung des Sicherheitskonzepts sowie die Wirksamkeitstests.



Über den Autor

Niels Lepperhoff

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

► www.xamit.de



BESCHÄFTIGTENDATENSCHUTZ UNTER DS-GVO & BDSG (NEU)

Thomas Kahl, Rechtsanwalt, Taylor Wessing

Was ändert sich für Unternehmen – was ist (jetzt) zu tun?

Mit Beschluss vom 12. Mai 2017 hat der Bundesrat dem am 05. Juli 2017 verkündeten Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) und dem darin enthaltenen BDSG (neu) zugestimmt und somit den Weg für verschiedene Anpassungen der DS-GVO in Deutschland geebnet.

1. Beschäftigtendatenschutz – Kernthema im DS-GVO Implementierungsprojekt

Mit § 26 BDSG (neu) macht der Gesetzgeber von der in Art. 88 DS-GVO vorgesehenen Möglichkeit Gebrauch, spezifischere Regelungen für den Beschäftigtendatenschutz auf nationaler Ebene zu erlassen, die Rechts- und Compliance-Abteilungen, Datenschutzbeauftragte und insbesondere HR-Teams vor einige Herausforderungen stellen werden.

Auch wenn erfreulicherweise mehr und mehr Unternehmen die Umsetzung der DS-GVO in Angriff nehmen – laut aktueller Zahlen des BITKOM beschäftigen sich zumindest über 40% der Unternehmen in den »digitalen« Branchen mit den neuen Regelwerken – zeigen die Erfahrungen in der Beratungspraxis, dass der Bereich des Beschäftigtendatenschutzes im Rahmen laufender DS-GVO-Projekte gerne hinten angestellt wird. Dabei sollte bei der Umsetzung der DS-GVO aus folgenden Gründen besonderes Augenmerk auf den HR-Bereich gelegt werden:

Erstens erfordern die tatsächlich wie rechtlich oft hoch komplexen Datenverarbeitungsprozesse eine meist aufwendige (Vorab-) Analyse, bevor überhaupt mit der eigentlichen »GAP-Analyse« und Anpassung an die neuen Vorgaben begonnen werden kann. Zweitens besteht das »Kerngeschäft« von HR-Abteilungen gerade in der umfassenden Verarbeitung oft sensibler personenbezogener Daten (z. B. Gesundheitsdaten i. H. a. Schwerbehinderung oder Religionszugehörigkeit für Steuer-Themen). Dabei werden in der DS-GVO und den ersten Guidelines der Art.-29-Gruppe (zukünftig Europäischer Datenschutz-

ausschuss) Verarbeitungsprozesse mit Beschäftigtendaten als besonders sensibel eingestuft (z. B. im Rahmen der Pflicht zur Durchführung eines Privacy Impact Assessments, »PIA«), so dass schon aus diesem Grund ein besonderer Fokus auf den HR-Bereich geboten ist. Drittens erschweren einzelne Sonderregelungen in § 26 BDSG (neu) die Erhebung und Verarbeitung von Beschäftigtendaten für Unternehmen in Deutschland. Dies hat zur Folge, dass grenzüberschreitende Konzepte für den Beschäftigtendatenschutz z. B. in internationalen Unternehmensgruppen nur mit Einschränkungen umsetzbar sein werden. Last but not least bleibt zu beachten, dass Anpassungen der Datenverarbeitungsprozesse und -konzepte im Zuge eines DS-GVO-Projekts ggf. der Mitbestimmung von Kollektivgremien unterliegen können. Da die hierzu erforderlichen Prozesse (z. B. Abschluss oder Neuverhandlung einer Betriebsvereinbarung) ein zeitaufwändiges Unterfangen sein können, sind betroffene Unternehmen gut beraten, entsprechende Vorgänge zu priorisieren, damit die rechtzeitige Umsetzung nicht an den erforderlichen Mitbestimmungsmaßnahmen scheitert.

2. Beschäftigtendatenschutz – Was bringt § 26 BDSG (neu)?

Die grundsätzliche Zulässigkeit der Verarbeitung von Beschäftigtendaten bestimmt sich zukünftig nach § 26 BDSG (neu). Die Norm folgt erkennbar der Struktur des § 32 BDSG und den hierzu anerkannten Grundsätzen, so dass die tatsächlichen materiell-rechtlichen Änderungen überschaubar sind. Die Norm enthält jedoch einige der DS-GVO geschuldete Klarstellungen, insbesondere die Möglichkeit der Einwilligung als Steuerungsinstrument im Beschäftigungsverhältnis und die Kollektivvereinbarung als (weiterhin) taugliche Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten.

Die Einwilligung im Beschäftigungsverhältnis ist grundsätzlich schriftlich zu erteilen, was die Umsetzung internationaler Konzepte im Umgang mit Beschäftigtendaten (z. B. Einwilligung zur Veröffentlichung von Fotos im Unternehmensintranet) erheblich erschwert. Mag die Regelung auf den ersten Blick wegen der Abweichung vom Grundsatz



der Formfreiheit für Einwilligungen (vgl. Art. 7 DS-GVO) verwundern, bleibt zu beachten, dass die Regelung der aktuellen Rechtsprechung des Bundesarbeitsgerichts (BAG) und der bisherigen Sichtweise der Aufsichtsbehörden folgt. Mag sich zukünftig der EuGH mit der Frage der Zulässigkeit dieser »Verschärfung« befassen, werden sich Unternehmen in Deutschland bis auf Weiteres an diese strengen Vorgaben halten müssen, was zu einem erheblichen administrativen Mehraufwand führen wird.

»Freiwillig« und somit wirksam sollen Einwilligungen des Beschäftigten u. a. dann sein, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigter gleichgelagerte Interessen verfolgen. Typische Einwilligungslösungen im Rahmen der Erlaubnis der Privatnutzung von E-Mail und Internet dürften somit auch (weiterhin) möglich bleiben. Andere Fallgestaltungen wie Einwilligungen im Rahmen des Recruitment-Prozesses (z. B. zur dauerhaften Speicherung von Bewerberdaten) dürften jedoch im Hinblick auf die neuen Anforderungen zu überprüfen und je nach Einzelfall anzupassen sein.

Entgegen der weit verbreiteten Praxis sind Beschäftigte zukünftig auch ausdrücklich auf das Widerrufsrecht hinzuweisen. In Zusammenschau mit den deutlich verschärften formalen Anforderungen an Einwilligungen (vgl. Art. 7 DS-GVO; Stichwort »aktive« Erklärungshandlung) werden somit alle Unternehmen ihre Einwilligungen überprüfen und anpassen müssen. Zu beachten bleibt, dass die Neuerungen bereits heute faktische Wirkung entfalten, da nur den neuen Vor-

gaben entsprechende Einwilligungen ab dem 25. Mai 2018 wirksam bleiben und deshalb »Altprozesse« so schnell wie möglich nachgezogen werden sollten.

An Tarifverträge, Betriebsvereinbarungen und andere Kollektivvereinbarungen stellen BDSG (neu) und DS-GVO hohe Anforderungen, ohne besondere Ausnahmen oder zusätzliche Übergangsregelungen für »Altfälle« vorzusehen. Kollektivvereinbarungen haben deshalb ab dem 25. Mai 2018 der neuen Rechtslage zu entsprechen, so dass auf die Betriebsparteien (Arbeitgeber, Legal, Compliance, HR und Kollektivgremien) viel Arbeit zukommen wird, um insbesondere die neuen Transparenzanforderungen gemäß Art. 13, 14 DS-GVO und den ergänzenden Vorgaben des Art. 88 DS-GVO rechtzeitig gerecht zu werden.

3. Was ist in der DS-GVO für den HR-Datenschutz besonders relevant?

Neben den Anforderungen des § 26 BDSG (neu) dürfen die »allgemeinen« Vorgaben der DS-GVO nicht aus dem Auge verloren werden:

Die prominenten Regelungen der Betroffenenrechte und insbesondere das Auskunftsrecht (Art. 15 DS-GVO) werden (wohl) zu einem erhöhten Aufkommen an entsprechenden Anfragen bestehender und ehemaliger Mitarbeiter führen. Um zusätzlichen administrativen Aufwand für ohnehin notorisch überlastete HR-Abteilungen zu vermeiden, sollten Unternehmen bereits jetzt ihre Systeme und Prozesse daraufhin prüfen, ob große Zahlen an Auskunftsanfragen zukünftig effektiv bedient werden können und ggf. »nachrüsten«.

Auf Grund der Sensibilität der Verarbeitung von Beschäftigtendaten dürften viele der gegenwärtigen und neuen HR-Prozesse zudem einem PIA zu unterziehen sein, dass entsprechend den neuen Vorgaben ausreichend zu dokumentieren und – im Ernstfall – sogar den Aufsichtsbehörden vorzulegen ist. Auch hierfür gilt: Es gibt keine Ausnahmen für Altfälle. Verfahren, die bereits existieren und ab 25. Mai 2018 weiterhin betrieben werden, sind entsprechend zu überprüfen. Bestehende Prozesse sollten schon wegen der eingangs beschriebenen tatsächlichen und rechtlichen Komplexität im HR-Bereich rechtzeitig betrachtet und angepasst werden, um ab Mai 2018 eine

lückenlose Dokumentation zu allen HR-relevanten Verfahren (vgl. Art. 30 DS-GVO) vorweisen zu können. Dies gilt ebenso für die Verarbeitung von Beschäftigtendaten außerhalb von elektronischen Systemen oder Dateisystemen (vgl. §26 Abs.7 BDSG [neu]), was im Rahmen der Dokumentation oft nicht oder nur unzureichend beachtet wird (z. B. wenn einzig eine technische Dokumentation auf »Application«-Basis erstellt wird). Die Informationspflichten gemäß Art. 13, 14 DS-GVO dürften in den meisten Unternehmen derzeit nur unzureichend umgesetzt sein. Deshalb sollten neben bestehenden Betriebsvereinbarungen (siehe hierzu bereits zuvor) alle im Unternehmen bestehenden Policies und Guidelines anhand der neuen Vorgaben geprüft und ergänzt werden.

Da gerade im Bereich HR vielfach mit externen Dienstleistern zusammengearbeitet wird (z. B. mit Betreibern von Personalmanagementsystemen, Payroll-Dienstleistern, Agenturen etc.), werden entsprechende Daten oft auf Basis von Vereinbarungen zur Auftragsdatenverarbeitung ausgetauscht (§11 BDSG). Art. 28 DS-GVO bringt einige Neuerungen für den Bereich der Auftragsdatenverarbeitung, die dazu führen, dass alle bestehenden Verträge zu prüfen und rechtzeitig anzupassen sind. Wegen der Neuordnung der Verantwortlichkeiten und Haftung der Auftragsdatenverarbeitung ist damit zu rechnen, dass die Neuverhandlungen – anders als in der Vergangenheit – ggf. aufwändiger werden, was bei der DS-GVO-Umsetzungsplanung maßgeblich zu berücksichtigen ist.

4. Datentransfer im Konzern – was erlauben DS-GVO & BDSG (neu)?

Ein »echtes« Konzernprivileg kennen weder die DS-GVO noch BDSG (neu). Erwägungsgrund Art. 48 DS-GVO dürfte aber eine gewisse Erleichterung beim Austausch von Beschäftigtendaten in Unternehmensgruppen bringen, was zu begrüßen ist. Danach können Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse daran haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Im Rahmen einer Interessenab-

wägung gemäß Art. 6 (f) DS-GVO dürften danach zukünftig einzelne Verarbeitungsprozesse wie z. B. die Übermittlung von Mitarbeiterdaten an eine Konzernmutter zum Zweck der Verarbeitung in einem zentralen HR-Managementsystem, das technisch durch die Muttergesellschaft betrieben wird, zulässig sein, wenn und soweit dies zu »internen Verwaltungszwecken« erfolgt. Auch wenn weiterhin erforderliche Garantien für den Transfer von Beschäftigtendaten in Drittstaaten im Sinne der Art. 44ff. DS-GVO vorliegen müssen, dürften in entsprechenden Fällen u. a. gesonderte Einwilligungen entbehrlich sein, was zu erheblicher Vereinfachung führen würde. Es bleibt jedoch abzuwarten, wie sich der Europäische Datenschutzausschuss und die deutschen Aufsichtsbehörden zu diesen Fragen positionieren und zu hoffen, dass sich die beschriebenen und längst überfälligen Erleichterungen zu Gunsten der Unternehmen in Deutschland durchsetzen.

5. Was Unternehmen jetzt tun müssen – Eine Checkliste für Legal, HR und den DSB

Wie gesehen, bringen die DS-GVO und BDSG (neu) neben Altbekanntem einige Neuerungen beim Beschäftigtendatenschutz, deren Umsetzung Legal & HR-Teams vor Herausforderungen stellen werden. Neben den gestiegenen Compliance-Risiken mit Bußgeldobergrenzen von bis zu 20 Mio. Euro oder 4% des weltweiten Vorjahresumsatzes des Unternehmens dürften insbesondere die formalen Anforderungen sowie Vorgaben zur Dokumentation und Accountability enormen Anpassungsaufwand im Unternehmen erzeugen, der bei der Zeit-, Budget- und Ressourcenplanung angemessen zu berücksichtigen ist.

Folgende Schritte sind deshalb jetzt erforderlich:

- Unternehmen müssen mit den Verantwortlichen Fachabteilungen (Legal, Compliance, HR und DSB) ein Konzept inkl. Timeline & Actionplan zur Umsetzung der DS-GVO erarbeiten.
- Hierzu sollten geeignete Verantwortliche aus dem Bereich HR benannt werden, um das Projekt im Hinblick auf die hohe Komplexität im HR-Bereich effektiv steuern und unterstützen zu können.

- Im Zuge des sog. »Data Mappings« sind alle relevanten HR-Datenverarbeitungsprozesse, verwendete Systemlandschaft(en) und TOMs zu ermitteln und ausreichend zu dokumentieren.
- Im Rahmen der rechtlichen Prüfung sollte besonderes Augenmerk auf die Zweckmäßigkeit und Rechtskonformität bestehender Einwilligungslösungen gelegt werden. Die Konzepte sind umgehend anzupassen, um »Doppelarbeit« zu vermeiden.
- Alle relevanten Kollektivvereinbarungen sind zu sichten und zu überprüfen. Anpassungsprozesse sind zeitnah einzuleiten, wobei die rechtliche Prüfung und Erarbeitung von Alternativkonzepten der Abstimmung mit Kollektivgremien vorausgehen sollte, um eine effektive und zügige Umsetzung zu gewährleisten.
- Auf Grund der gestiegenen Bedeutung der Betroffenenrechte sind alle hierzu bestehenden Prozesse zu prüfen und auf den neuen Stand zu bringen.
- AV-Vereinbarungen mit HR-Bezug sind vor Mai 2018 zu überarbeiten.
- Last but not least sind alle HR-Policies und Guidelines den erweiterten Informationspflichten anzupassen.

Long story short: Der Weg ist (noch) weit – die Zeit ist kurz. Zielsetzung jedes Unternehmens sollte es sein, ab Mai 2018 das Compliance-Management System (CMS) um die neue »Säule« Datenschutz ergänzt zu haben. In Abstimmung mit den betroffenen Abteilungen sind dafür zukunftsfähige und praxisnahe Konzepte zu entwickeln, die im Unternehmensalltag effektiv eingesetzt werden können.

Um dieses Ziel rechtzeitig zu erreichen, müssen sich Unternehmen jetzt mit den Neuerungen insbesondere beim Beschäftigtendatenschutz befassen. Denn auch wenn die materiellen Änderungen in diesem Bereich durchaus überschaubar sind, zwingen nicht zuletzt die gestiegenen formalen Anforderungen zu umfangreichen Anpassungen im HR-Bereich, um am 25. Mai 2018 »compliant« aufgestellt zu sein.

Über die Autoren

Thomas Kahl

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



Anzeige

PROCILON
GROUP

SecurITy

Trust Seal
www.eletrust.de/itsmg

made
in
Germany

SICHER

identifizieren



kommunizieren



aufbewahren



Informationssicherheit und Datenschutz aus einer Hand

DATENSCHUTZ-RISIKOMANAGEMENT

Dipl.-Ök. Stephan Rehfeld

Bei dem Aufbau eines Datenschutz-Managementsystems ist die Prägung des Managementsystems auf die Datenschutz-Grundsätze der Datenschutz-Grundverordnung (DS-GVO) ein erfolgsentscheidender Faktor. Nur wenn alle Datenschutz-Grundsätze der DS-GVO in das Managementsystem eingearbeitet sind, kann das Datenschutz-Managementsystem die Organisation vor Datenschutzverstößen schützen. Bei der Einarbeitung der Datenschutz-Grundsätze ist zu klären, welchen Umfang ein gefordertes Datenschutz-Risikomanagement hat, also welche Datenschutz-Grundsätze überhaupt risikoorientiert sind.



Datenschutz-Grundsätze

Die Datenschutz-Grundverordnung kennt verschiedene Grundsätze für die Verarbeitung von personenbezogenen Daten:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Artikel 5 Abs.1 lit. a)
- Zweckbindung, Artikel 5 Abs.1 lit. b)
- Datenminimierung, Artikel 5 Abs.1 lit. c)
- Richtigkeit, Artikel 5 Abs.1 lit. d)
- Speicherbegrenzung, Artikel 5 Abs.1 lit. e)
- Integrität und Vertraulichkeit, Artikel 5 Abs.1 lit. f)
- Rechenschaftspflicht, Artikel 5 Abs.2

Bis auf die Betroffenenrechte können alle Artikel der Kapitel 2–5 der DS-GVO unter diese Datenschutz-Grundsätze subsumiert werden. Eine Ergänzung dieses Kanons um den Datenschutz-Grundsatz für die Betroffenenrechte wie »Persönliche Teilhabe und Zugang« wurde vom europäischen Gesetzgeber anscheinend »vergessen«. Andere Rahmenwerke zum Datenschutz wie das OECD Privacy Framework oder auch die ISO 29100:2011 führen einen solchen Grundsatz explizit auf (»Individual Participation Principle«). Aus Gründen der Praktikabilität empfiehlt es sich die »Persönliche Teilhabe und Zugang« in den Kanon der Grundsätze für das eigene Managementsystem zu übernehmen. ▶

Datenschutz-Managementsystem

Fast alle aktuellen Management-Systeme der International Organization for Standardization (ISO) orientieren sich in ihrem Aufbau an der High Level Structure (HLS), die in dem ISO Guide 83¹ beschrieben ist. Die Struktur eines Qualitäts- (ISO 9001), Umwelt- (ISO 14001) oder Informationssicherheits-Managementsystems (ISO 27001) ist also identisch. Die konkrete Ausprägung des Managementsystems wird durch die zugrundeliegenden Grundsätze bestimmt. Beispielhaft seien hier die Grundsätze eines Datenschutz- und eines Informationssicherheits-Managementsystems gegenübergestellt:

Datenschutz-Managementsystem (DSMS)	Informationssicherheits-Managementssystem
<ul style="list-style-type: none"> • Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Artikel 5 Abs.1 lit. a) • Zweckbindung, Artikel 5 Abs.1 lit. b) • Datenminimierung, Artikel 5 Abs.1 lit. c) • Richtigkeit, Artikel 5 Abs.1 lit. d) • Speicherbegrenzung, Artikel 5 Abs.1 lit. e) • Integrität und Vertraulichkeit, Artikel 5 Abs.1 lit. f) • Rechenschaftspflicht, Artikel 5 Abs.2 • Persönliche Teilhabe und Zugang 	<ul style="list-style-type: none"> • Vertraulichkeit • Integrität • Verfügbarkeit

Generell ist es also möglich, jedes Management-system, welches auf der High Level Structure basiert, mit einem Datenschutz-Management-system zu kombinieren, indem es durch die Datenschutz-Grundsätze und deren Implikationen erweitert wird. Dies ist auch ein Grund, warum die ISO kein eigenes Datenschutz-Management-system erarbeiten wird, stattdessen empfiehlt, ein Informationssicherheits-Managementssystem auf Basis der ISO/IEC 27001:2013 an den Datenschutz anzupassen. Für diese Anpassung wiederum gibt die ISO Hilfestellung, zum Beispiel mit einem Leitfaden zum PIA (ISO/IEC 29134:2017) oder datenschutzspezifischen Maßnahmenkatalogen (ISO/IEC 27018:2014 und ISO/IEC FDIS 29151:2016).

¹ https://share.ansi.org/Shared%20Documents/News%20and%20Publications/Links%20Within%20Stories/Draft_ISO_Guide_83.pdf

² RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (23 September 1980)

³ <https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf>

Risikoorientierter Ansatz in der DS-GVO

Wenn von dem risikoorientierten Ansatz der DS-GVO geschrieben wird, muss die Frage gestellt werden, welche Datenschutz-Grundsätze risikoorientiert sind.

Die Datenschutz-Grundsätze oder -Prinzipien sind keine Erfindung der DS-GVO. Sehr frühe Ansätze der Datenschutz-Grundsätze finden sich bereits in den OECD-Principles aus dem Jahr 1980.² Die OECD-Principles dienen auch zur Definition weltweit einheitlicher Datenschutz-Standards aus einer High-Level-Perspektive. Folgende Datenschutz-Grundsätze verwendet die OECD:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

Die OECD Privacy Principles sind in viele nationale Gesetze eingeflossen. Sie wurden allerdings nicht unter dem Aspekt der Risikoorientierung oder der Konkurrenz der Grundsätze untereinander ausgewählt.

Auf der einen Seite gibt es Datenschutz-Grundsätze mit einem binären Charakter, zum Beispiel die Rechtmäßigkeit. Ein Sachverhalt kann nur rechtmäßig oder nicht rechtmäßig sein. Der Grundsatz der Rechtmäßigkeit kann aber nicht risikoorientiert ausgelegt werden (der Sachverhalt ist mit einer Wahrscheinlichkeit von 80% rechtmäßig). Aus diesem Grund werden die Datenschutz-Prinzipien in dem Bitkom-Leitfaden zum Risk-Assessment und zur Datenschutz-Folgenabschätzung³ in zwei Lager unterteilt:

Der Datenschutz-Grundsatz der Rechenschaftspflicht wiederum begleitet beide Sichtweisen.

Die Datenschutz-Grundsätze der Compliance-Sicht sind nicht risikoorientiert, anders als die Grundsätze der Risiko-Sicht.

Compliance-Sicht	Risiko-Sicht
<ul style="list-style-type: none"> • Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Artikel 5 Abs.1 lit. a) • Zweckbindung, Artikel 5 Abs.1 lit. b) • Datenminimierung, Artikel 5 Abs.1 lit. c) • Richtigkeit, Artikel 5 Abs.1 lit. d) • Speicherbegrenzung, Artikel 5 Abs.1 lit. e) 	<ul style="list-style-type: none"> • Integrität und Vertraulichkeit, Artikel 5 Abs.1 lit. f)

International wird diese Auffassung geteilt und auch praktisch umgesetzt. So unterteilt die französische Aufsichtsbehörde (CNIL) ihren Maßnahmen-Katalog⁴ in Maßnahmen (controls), die den Datenschutz-Grundsätzen der Compliance-Sicht zugeordnet werden können (Legal controls) und denen, die der Risiko-Sicht zugeordnet werden können (Organizational controls, Logical security controls, Physical security controls).

In dem Maßnahmen-Katalog wird von der CNIL darauf hingewiesen, dass die Legal controls verpflichtend (mandatory) sind und erfüllt werden müssen, während die risikoorientierten Maßnahmen einer Risikobehandlung unterzogen werden:

- Risikovermeidung
- Risikominderung
- Risikoanerkennung
- Risikoakzeptanz

Die Optionen der Risikobehandlung sind bei den binären Datenschutz-Grundsätzen der Compliance-Sicht logischerweise nicht möglich.

Datenschutz-Risikomanagement

Bei der Einrichtung eines Datenschutz-Risikomanagements gibt die ISO 31000:2009 wertvolle Hinweise. Auf der einen Seite empfiehlt es sich auf Ebene des Management-Systems das Datenschutz-Risikomanagementsystem mit Hilfe einer Datenschutzrisiko-Leitlinie zu verankern. Ist bereits ein ISO 31000- oder ISO 27005-konformes Risikomanagement vorhanden sollte auf jeden Fall eine Integration der Systeme vorgenommen werden.

Der eigentliche Datenschutz-Risikomanagementprozess ist mit dem allgemeinen Risikomanagementprozess identisch und besteht aus fünf Schritten:

- Risiken identifizieren
- Risiken analysieren
- Risiken bewerten
- Risiken bewältigen
- Risiken überwachen

Zur eigentlichen Methodik zur Berechnung des Datenschutzrisikos werden in der DS-GVO nur sehr wenige Ausführungen gemacht. Diese Freiheit in der Auswahl der Risikomethode zur Berechnung des Datenschutzrisikos ist auch richtig, wenn die Anzahl der Methoden in der ISO/IEC 31010:2009 betrachtet wird. Bei der Auswahl der Risikomethode müssen lediglich die gesetzlichen Restriktionen beachtet werden, die auch die Artikel 29-Gruppe in ihrem Working Paper⁵ nennt:

Risks can change as a result of change to one of the components of the processing operation (data, supporting assets, risk sources, potential impacts, threats, etc.) or because the context of the processing evolves (purpose, functionalities, etc.). Data processing systems can evolve quickly and new vulnerabilities can arise.

Diese Anforderungen werden durch die Methodiken erfüllt, die zum Beispiel die CNIL⁶, der Bitkom⁷ oder auch die ISO⁸ beschreibt.

⁴ CNIL, Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf>

⁵ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is «likely to result in a high risk» for the purposes of Regulation 2016/679, http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Fazit

Für den Aufbau eines Datenschutz-Managementsystems ist die Prägung des Managementsystems auf alle Datenschutz-Grundsätze der DS-GVO erfolgsentscheidend. Es sollte in Betracht gezogen werden, die Datenschutz-Grundsätze des Artikel 5 DS-GVO durch den Grundsatz der »Persönlichen Teilhabe und des Zugangs« zu ergänzen, also auch die Betroffenenrechte mit Hilfe der Datenschutz Grundsätze operationalisierbar zu machen.

Bei der Implementierung des Datenschutz-Risikomanagements ist es wichtig zu verstehen, dass nicht alle Datenschutz-Grundsätze risikoorientiert sind. Nur die Datenschutz-Grundsätze der Vertraulichkeit und Integrität sind risikoorientiert.

Ergänzt werden diese beiden Grundsätze in Artikel 28 DS-GVO dann noch durch die Verfügbarkeit und Belastbarkeit. Andere Grundsätze haben einen binären Charakter und können nur verletzt oder eingehalten werden.

⁶ CNIL, Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf>

⁷ Bitkom, Leitfaden zum Risk-Assessment und zur Datenschutz-Folgenabschätzung, <https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf>

⁸ ISO/IEC 29134:2017, Information technology – Security techniques – Guidelines for privacy impact assessment

Über den Autor



Stephan Rehfeld

Externer Datenschutzbeauftragter der scope & focus Service-Gesellschaft mbH

► www.scope-and-focus.com



Anzeige



DATENSCHUTZ

SAP SECURITY

INFORMATIONSSICHERHEIT

IT-SECURITY

Datenschutz-Manager

Das Datenschutzmanagementsystem für den DSB – gemäß DS-GVO

- > 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 zur Erfüllung der Anforderungen zur Rechenschaftspflicht
- > Verzeichnis von Verarbeitungstätigkeiten mit **mehr als 150 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



Anerkannte Prüfstelle für Recht und Technik beim ULD für das Datenschutz-Gütesiegel



DATENSCHUTZ-GRUNDVERORDNUNG - EINE SINNVOLLE HERAUSFORDERUNG ODER PROVOKATION FÜR KLINIKEN UND KRANKENHÄUSER?

Dr. jur. Siegfried Meyer

Die komplexen Verarbeitungsprozesse in einer digitalen Multimedia-Welt mit der Anbindung an ein weltweites Internet, zunehmende Cyber-Angriffe auf Krankenhäuser und die große Bedeutung von »Big Data« im 21. Jahrhundert lassen die Vereinheitlichung des europäischen Datenschutzrechts als wichtigen und sinnvollen Schritt europäischer Integration verstehen.

Altbekannte Datenschutzgrundsätze in der DS-GVO

Auf den ersten Blick kann man viele Datenschutzgrundsätze in der Datenschutz-Grundverordnung der EU (DS-GVO) wiedererkennen. Das Verbot mit Erlaubnisvorbehalt im alten BDSG, die Zweckbindung, die Grundsätze der Datensparsamkeit und der Transparenz, sowie die Grundsätze der Verhältnismäßigkeit, der Ver-

fügbareit und Vertraulichkeit finden sich auch in der neuen DS-GVO wieder. Gleiches gilt etwa für die Rechte der Betroffenen, wie etwa das Recht auf Auskunft, Sperrung, Löschung oder Berichtigung (vgl. Art 15 bis Art 20 DS-GVO).

Weiterhin gab es auch bereits bisher fest geregelte Anforderungen an die sogenannten technisch-organisatorischen Maßnahmen (TOMs) wie sie in §9 und Anlage 9 zum BDSG oder Art. 7 BayDSG geregelt waren. Diese Regelungen können wir nun in den Artikeln 24, 25, 28, 32 DS-GVO wieder finden. Schließlich mussten auch bisher Datenschutzverletzungen nach §42a BDSG unverzüglich der Aufsichtsbehörde gemeldet werden, wenn gleichzeitig schwerwiegende Beeinträchtigungen für die Rechte oder für schutzwürdige Interessen des Betroffenen gedroht haben. ▶

Wunderbar, dann hat sich ja beim Schutz personenbezogener Daten und dem Schutz etwa von Gesundheitsdaten in den Krankenhäusern nicht viel geändert?

Neue Herausforderungen nach der DS-GVO für Kliniken und Krankenhäuser

Auf den zweiten Blick, selbst wenn man die konkretisierenden Regelungen im neuen BDSG noch nicht berücksichtigt, werden Anforderungen der DS-GVO zumindest im Bereich der Krankenhäuser und Kliniken zu neuen Herausforderungen führen! Einige neue Anforderungen und sicherlich einige Investitionen aufgrund der DS-GVO kommen unzweideutig auf die Kliniken und Krankenhäuser zu.

Bei der nur zum Teil sinnvollen Gesetzesflut, die wir täglich erleben, sollte nicht vergessen werden, dass mit zusätzlichen Regelungen in der Regel auch ein höherer Aufwand und damit Kosten verbunden sind, deren Gegenfinanzierung der jeweilige Gesetzgeber in der Regel übersieht. »Eine derartig umfassende Gesetzesänderung gibt es nicht zum Nulltarif«, wie Herr Dr. Bernd Schütz in seinem Interview mit Frau Melanie Günther [Quelle European Hospital, healthcare-in-europe.com] bestätigt. Der Patient oder der hier vom Datenschutz Betroffene soll stets im Mittelpunkt der Betrachtung und Behandlung stehen. Darin sind sich alle einig und dieses Ziel streben alle an. Der Patient und seine medizinische Versorgung sowie der Schutz seiner hochsensiblen Gesundheitsdaten, aber auch die Anforderung an die Wirtschaftlichkeit und Qualität der Versorgung stehen im Mittelpunkt, und das bei einer vom Gesetzgeber vorgegebenen (verkürzten) Verweildauer. Die Datenschutzrechte und deren Durchsetzbarkeit für den Patienten sollen durch den europäischen Datenschutz weiter verbessert werden. Es gibt allerdings schon eine Vielzahl von anderen Dokumentationsaufgaben und Nachweispflichten in den deutschen Krankenhäusern. Zu nennen sind die erhöhte Anforderungen an die Nachweispflicht im Qualitätsmanagement, aber auch die Anforderungen an die Patientenaufklärung (vgl. § 630e BGB) und an die Dokumentation (vgl. § 630f BGB) seien nicht zu vergessen.

Der Arzt, der Behandler oder das Krankenhaus, welche ihrer sorgfältigen Aufklärungs- und Dokumentationspflicht nicht nachkommen, müssen im Falle eines Rechtsstreits mit Nachteilen in der Beweislastverteilung rechnen (vgl. § 630h BGB).

Welche zusätzlichen Anforderungen bringt die DS-GVO für die Krankenhäuser und Kliniken?

An dieser Stelle seien beispielhaft

- die Rechenschaftspflicht aus Art 5 Abs.2 DS-GVO,
- die Anforderung nach einem lückenlosen Verzeichnis »aller« Verarbeitungstätigkeiten nach Art. 30 DS-GVO,
- die Datenschutz-Folgeabschätzung nach Art. 35 DS-GVO,
- die gesteigerten Meldepflichten nach Art. 33 und Art. 34 DS-GVO,
- die Anpassung der Auftragsdatenverarbeitung an die Anforderungen aus Art. 28 DS-GVO

genannt. Während man bisher bei der Verarbeitung durch externe Vertragspartner von Auftragsdatenverarbeitung gesprochen hat, spricht die DS-GVO in Art 28 DS-GVO nun von Auftragsverarbeitung. Während bisher die alleinige Verantwortung über die Verarbeitung personenbezogener Daten durch den externen Auftragnehmer nur bei dem Auftraggeber lag, ist nach der neuen DS-GVO auch der Auftragnehmer in die Verantwortung einbezogen. Die stärkere Einbeziehung des Auftragnehmers ist klar zu befürworten, denn in manchen Fällen sind insbesondere große Auftragnehmer insbesondere mit Monopolstellung etwa der im Bereich der Fernwartung von IT-Systemen und medizintechnischen Anlagen nicht immer motiviert, von Anfang an einen umfangreichen ADV-Verträge zur Sicherstellung der Auftragsdatenverarbeitung abzuschließen. Wenn die Anforderungen aus dem europäischen Datenschutzgesetz nicht erfüllt werden, drohen aber Maßnahmen der Aufsichtsbehörde und gemäß Art. 83 DS-GVO Bußgelder von bis zu 20 Mio.€ oder 4% des Jahresumsatzes, aber auch Schadensersatzansprüche (Art. 82 Abs.1 DS-GVO) oder

sonstige »abschreckende Sanktionen« strafrechtlicher oder verwaltungsrechtlicher Art. [vgl. Erwägungsgrund 152].

Das wäre an sich auch nicht so schlimm, denn die Krankenhäuser und Kliniken zeigen seit vielen Jahren, dass sie sich stets an neue gesetzliche Regelungen, etwa im Qualitätsmanagement, in der DRG-Vergütung (Honorierung der Krankenhäuser nach Fallpauschalen) oder in der staatlichen Baufinanzierung, im Haftungsrecht oder zuletzt in der IT-Sicherheit rasch anpassen können.

Bei dem hohen Bußgeldrahmen könnte aber eingewandt werden, dass die Strafbarkeit bei Verletzung der ärztlichen Schweigepflicht gemäß § 203 StGB auch bisher schon gedroht hat. Das ist richtig. Nur sollte man nicht vergessen, dass der Verantwortliche oder Auftragsverarbeiter nach Art. 82 Abs.2 DS-GVO nun aktiv nachweisen muss, dass er in »keinerlei Hinsicht« verantwortlich für den eingetretenen Schaden ist. Im Strafrecht muss das Verschulden des Beschuldigten von Ankläger nachgewiesen werden, in einem komplexen Verarbeitungsprozess mit einer Vielzahl von Personengruppen, Patientenzahlen und Gesundheitsdaten dürfte die in Art. 5 Abs.2 DS-GVO fixierte Rechenschaftspflicht nicht leicht zu erfüllen sein.

Ob ein derartiges Bedrohungsszenario durch einen extrem hohen Bußgeldrahmen im Sinne des Patienten ist, darüber lässt sich trefflich streiten! Werden tatsächlich die hohen Bußgelder zur Abschreckung ausgesprochen, dann fehlen diese Gelder in der Finanzierung eines komplexen stationären Versorgungsprozesses im Körpersektor, eine Daseins-Vorsorgeeinrichtung, die in weiten Teilen unterfinanziert wird. Ein Versorgungsprozess, der aber gerade den Patienten zugutekommen soll und mehr Geld gibt es sicher nicht.

Was gilt es nun zu tun, damit ein Vorstand oder Geschäftsführer eines Krankenhauses oder Klinikums kein abschreckendes Bußgeld für seine ohnehin unterfinanzierte Versorgungseinrichtung riskiert?

Es müssen m.E. zunächst in einem 1. Schritt alle IT-gestützten und papiergestützten Datenverarbeitungsprozesse und zwar über die

verschiedenen Abteilungen, Personengruppen, Anwendungen und IT-Infrastruktur-Komponenten hinweg mit den verschiedenen Datenarten (Patientenstammdaten, Gesundheitsdaten, Bilddaten, Bewerber- und Mitarbeiterdaten) aktualisiert erfasst werden. In einem 2. Schritt gilt es jeweils den Schutzbedarf festzustellen, und in einem 3. Schritt die korrekte Risikoeinstufung nach Schadenshöhe und Eintrittswahrscheinlichkeit vorzunehmen. Mit der Risikoeinstufung gilt es zu klären, ob jeweils auf das einzelne Verfahren oder auf die einzelne Applikation bezogen, die vorhandenen technische und organisatorische Maßnahmen (TOMs) ausreichen oder je nach Risikoeinstufung neu festgesetzt werden müssen.



Kommt es zu neuen Risikoeinstufungen, die einen Handlungsbedarf begründen, dann werden die nach den Schutzbedarfsanforderungen neuen IT-technischen Sicherheitsmaßnahmen und Investitionen getroffen werden müssen, um Schnittstellen nach Extern oder interne Schwachstellen bei den verschiedenen Anwendungen rasch aus der Welt zu schaffen. Wobei technische Verfahren zur Investitionen in die IT in der Regel teuer aber schnell umsetzbar sind. Organisatorische Verfahren müssen allerdings in die Köpfe und dafür bedarf es Schulung und Überzeugungsarbeit. Das alles muss selbstverständlich sorgfältig dokumentiert werden, damit die oben genannte Rechenschaftspflicht, aber auch mögliche Auskunftspflichten an die

Aufsichtsbehörden zum Mai 2018 rechtzeitig sichergestellt werden können. Das Ganze muss natürlich mit dem gleichen Personal und ohne zusätzliche finanzielle Forderung gemacht werden. Der Leistungsdruck wird weiter steigen! Ferner gilt es die vorhandenen Verträge mit den Auftrags(daten)verarbeitern (externen Dienstleistern, Fernwartern in der IT, Labore, etc.) an die neuen Anforderungen des Art. 28 DS-GVO anzupassen. In einem 4. Schritt muss ein einheitliches Verfahren im Krankenhauskomplex entwickelt werden, wie alle Datenschutzverletzungen binnen 72 Stunden gemäß Art. 33 Abs.1 DS-GVO an die zuständige Aufsichtsbehörde gemeldet werden kann.

Wer die komplexen Prozesse in einem modernen Krankenhaus kennt, weiß, wie viele Personengruppen (Ärzte, Pflegekräfte, Funktionsabteilungen, interne und externe Labore, IT, medizin- und haustechnische Serviceabteilungen, medizinisches Controlling und Abrechnung, Qualitätssicherung, Verwaltung und Hygiene) innerhalb kürzester Zeitfenster zusammenarbeiten müssen, um insbesondere auch in akuten Notfällen rasch de lege artis versorgen zu können.

Der Datenschutz und die IT-Sicherheit auf der einen Seite mit seinen nachzuweisenden TOMs und rasche qualitätsgesicherte Patientenversorgung auf der anderen Seite geraten so ein Spannungsverhältnis. Der Datenschutz und die ärztliche Schweigepflicht stehen den Anforderungen eines möglichst raschen und flexiblen Zugriffs der Ärzte verschiedener Abteilungen im komplexen Klinikalltag naturgemäß »gerne im Wege«. Nur dann, wenn der Arzt die Möglichkeit hat, ganz schnell auf alle Gesundheitsdaten seiner Patienten, gegebenenfalls auch aus früheren Krankenhausaufenthalten, zugreifen zu können, versetzt dies den Arzt in die Lage, das Krankheitsbild in der Kürze der vorgegebenen durchschnittlichen Verweildauer de lege artis zu beurteilen und zu therapieren. Kann er auf Patientenakten aus früheren Krankenhausaufenthalten nicht zugreifen, besteht die Gefahr, dass er sich und sein Klinikum haftbar macht, weil er wichtige Informationen im Rahmen des Behandlungskonzeptes vorwerfbar nicht beachtet hat.

Diejenigen Ärzte, welche beispielsweise in der zentralen Notaufnahme einen akuten Traumatpatienten mit verschiedenen Vor- und Begleiterkrankungen behandeln müssen, sollten sehr rasch auf alle vorhandenen Gesundheits- und Bilddaten des Patienten, ggf. aus früheren stationären Aufenthalten, zugreifen können. Ein Zugriff aller Ärzte auf alle Gesundheitsdaten aus früheren Krankenhausaufenthalten verbietet sich aber aus datenschutzrechtlichen Gründen, und die auftretenden Notfälle und Notfallpatienten - das liegt in der Natur der Sache - können nicht vorausgesehen werden. Wenn ich nicht weiß, wer von meinen früheren Patienten zukünftig als stationärer Notfall hereinkommt, dann kann ich für diesen Patienten den Notfallzugriff nicht vorab - gleichsam präventiv - freischalten. Denn das es würde den Grundsätzen der Datensparsamkeit und konkreten Erforderlichkeit widersprechen. Dabei gilt es zu beachten, dass die ärztliche Schweigepflicht auch zwischen den verschiedenen Arztgruppen in einem Krankenhaus gilt und so der ärztliche Kollege, der nicht in die Behandlung des Patienten eingebunden ist, auch von dem Patienten nichts erfahren darf, bis er im Behandlungsfall, beispielsweise als Konsiliarius, hinzugezogen wird.

Die Datenschutz-Anforderungen werden noch komplexer, wenn in akuten Versorgungsprozessen in der Notaufnahme, in denen rasches Handeln angesagt ist, auch noch besorgte Angehörige anwesend sind, die möglichst nahe bei ihren Familienangehörigen bleiben möchten und zugleich andere Akut-Patienten in ähnlicher Situation versorgt werden müssen. Auch und besonders in diesen Notfallsituationen gilt es, den Datenschutz und die ärztliche Schweigepflicht zu beachten. Gleichzeitig müssen aber die Anforderungen an die Aufklärung der Patienten und die Dokumentation der Aufklärung und Behandlung sorgfältig vorgenommen werden.

Da es leider noch keine einheitliche Multimedia-Anwendung in den Kliniken gibt, mit der alle medizinischen, technischen und pflegerischen Anforderungen IT-technisch abgebildet werden können, greifen an dieser Stelle auch verschiedene Hard- und Software-Komponenten mit den unterschiedlichen Rollen-/Rechtekonzepten für die Zugriffe ineinander. Zu allen Applikati-

onen muss es exakte Rollen-/Rechtekonzepte und deren technische Absicherung geben. Muss ein multimorbider Patient wegen seines Krankheitsbildes durch verschiedene Abteilungen und Kliniken verlegt werden, um optimal innerhalb der gesetzlich vorgegebenen Verweildauer behandelt werden zu können, dann müssen die Zugriffsrechte blitzschnell geändert werden.

Zur Klarstellung: Technischen und organisatorischen Maßnahmen mit den verschiedenen Rollen-Rechtekonzepten für den Datenschutz und IT-Sicherheitskonzepte gibt es bereits. Die Frage ist nur, ob man damit der in der DS-GVO geforderten Rechenschaftspflicht und den damit zwangsläufig verbundenen Dokumentationspflichten gerecht werden kann, so dass einerseits Risiken für den Patienten vermieden werden und andererseits die abschreckenden Sanktionen nicht zur Anwendung kommen.

In Zeiten, in denen große Datenmengen verarbeitet werden und im Internet auf den verschiedenen Plattformen gesammelt und ausgewertet werden und mithin die Gefahr des gläsernen Bürgers besteht, ist ein europaweites und strenges Datenschutzrecht in jedem Fall zu begrüßen. Es stellt sich allerdings die Frage, ob die »abschreckenden« Sanktionen bei der Vielzahl der anderen Regelungsvorschriften, die im Gesundheitswesen einzuhalten sind, dem Patienten im Ergebnis noch dienen? Im Einzelfall lässt sich wieder feststellen, dass die Regelung und Vorschriften in den verschiedenen Bereichen für sich sinnvoll sind, in der Gesamtbetrachtung mit

zum Teil gegensätzlichen Regelungszielen aber ein vernünftiges Arbeiten nicht mehr möglich machen!

Der deutsche und europäische Gesetzgeber sollte sich vielmehr in einer Gesamtbetrachtung die Frage stellen, ob nicht weniger Regelungen dem Wohl des Bürgers in einer freiheitlichen und demokratischen Grundordnung gerechter würde. Die Vielzahl der Vorschriften und Regelungen auch im Datenschutz (vgl. DS-GVO, neues BDSG; BayDSG, SGB V, etc.) entmündigt den gesunden Menschenverstand der betroffenen Personen und »freien« Bürger, für den sie an sich gedacht waren. Planwirtschaft im Gesundheitswesen lässt grüßen!

Ich würde mir wünschen, dass die Ärzte und alle nichtärztlichen Mitarbeiter vom deutschen und europäischen Gesetzgeber weniger Verfahrens- und Rechenschaftspflichten ausgesetzt würden, damit weit weniger Dokumentationsaufwand hätten und somit wieder mehr Zeit und Geld für die eigentliche Versorgung am Patienten verbliebe. Das würde zugleich noch Kosten im Gesundheitswesen einsparen!



Über den Autor

Dr. jur. Siegfried Meyer

Justiziar und Leiter der Rechtsabteilung am Klinikum St. Marien Amberg und Prokurist im Gesundheitszentrum St. Marien GmbH (MVZ) und Mitglied in der Arbeitsgruppe »Datenschutz« der BKG (Bayerischen Krankenhausgesellschaft).

Anzeige



ISO 27001
Informationssicherheit
für Unternehmen



ERKLIMMEN SIE DIE KARRIERELEITER

Investieren Sie zukunftsweisend in die Informationssicherheit Ihrer Organisation und lassen Sie sich von uns zum zertifizierten ISO/IEC 27001-Experten schulen:

- ISO 27001 FOUNDATION
- ISO 27001 OFFICER
- ISO 27001 AUDITOR

IHRE QUALIFIZIERUNG DURCH UNSERE ZERTIFIZIERUNG!



FOUNDATION
18.09. - 19.09.2017
13.11. - 14.11.2017

OFFICER
20.09. - 22.09.2017
15.11. - 17.11.2017

AUDITOR
27.09. - 29.09.2017
22.11. - 24.11.2017



Weitere
Informationen:

DS-GVO WEITET DOKUMENTATIONS- PFLICHTEN DEUTLICH AUS

Datenschutzmanagement wird zu dynamischem Prozess,
der alle Unternehmensbereiche umfasst

Die Europäische Datenschutzgrundverordnung (DS-GVO) bringt erweiterte Anforderungen an die Datenschutz-Dokumentation mit sich. »Wer sich allerdings nur den Verordnungstext vornimmt und nachliest, welche Dokumente gefordert sind, springt deutlich zu kurz«, warnt Christian Volkmer, Inhaber des Regensburger Datenschutz-Spezialisten Projekt 29.



Christian Volkmer,
Projekt 29 GmbH & Co. KG

den in verschiedenen Artikeln der Verordnung ausdrücklich geforderten Dokumenten eine ganze Reihe weiterer Dokumente und Aufzeichnungen stets aktuell vorhalten. Gut zusammengefasst findet sich eine Aufstellung in Kapitel 7 des E-Books »Datenschutz-Compliance nach der DS-GVO« (Bundesanzeiger Verlag, ISBN 978-3-8462-0773-4), das der Präsident des Bayerischen Landesamtes für Datenschutzaufsicht Thomas Kranig und Andreas Sachs, Leiter des technischen Referats der Behörde, mitverfasst haben.

Ständige Kontrolle und Verbesserung

Wie im Qualitätsmanagement nach ISO 9001 oder im IT-Sicherheitsmanagement nach ISO 27001 gefordert, muss künftig auch das Datenschutzmanagement zyklisch nach der PDCA-Methode ständig aktualisiert werden. »P« steht für das englische »plan«, also planen. Dieser Schritt entspricht noch am ehesten dem gewohnten Verfahrensverzeichnis. »Als Verfahren wird aufgeschrieben, was passieren muss, wenn zum Beispiel ein Kunde im Callcenter anruft und verlangt, dass seine Daten gelöscht werden«, sagt Volkmer. »D« steht für »do«, also die konkrete Umsetzung des Löschersuchens. »Hier entsteht eine neue Dokumentationspflicht«, so Volkmer. Aufgezeichnet werden muss sowohl, dass ein Kunde die Löschung verlangt hat als auch dass das Unternehmen diesem Ersuchen nachgekommen ist.

»Die EU-Verordnung wird den Alltag von Datenschutz-Verantwortlichen komplizierter machen«, sagt Volkmer voraus. Denn es geht um deutlich mehr, als die Ablösung des Verfahrenszeichnisses nach Bundesdatenschutzgesetz (BDSG) durch ein erweitertes Verfahrensverzeichnis. »Die DS-GVO fordert einen dynamischen Prozess, der die Datenschutzpraxis im Unternehmen immer wieder überprüft und nachbessert. Dieser dynamische Prozess muss lückenlos dokumentiert werden«, sagt der Experte. Deswegen müssen Unternehmen neben

»C« meint »check«, in unserem Beispiel die Überprüfung, dass Löschersuchen tatsächlich in allen Fällen korrekt erfasst und umgesetzt werden, was wiederum dokumentiert werden muss. Fällt dabei auf, ob doch nicht alles korrekt läuft, gilt »A« oder »act«: Der im ersten Schritt gefasste Plan, das Verfahren, muss korrigiert und das Verzeichnisse geändert werden.

»Das einfache, kleine Beispiel eines Löschersuchens zeigt eindrücklich, wie komplex die Dokumentation ab nächstem Jahr wird«, sagt Volkmer. Knifflig macht die Sache zusätzlich, dass Mängel an der Dokumentation nach BDSG nicht bußgeldbewehrt sind, nach DS-GVO allerdings schon. Und zwar mit der vollen Härte des Bußgeldrahmens von bis zu vier Prozent des Vorjahresumsatzes oder bis zu 20 Millionen Euro.

Aufsichtsbehörde empfiehlt Managementsystem

Mit Word- oder Exceldokumenten irgendwo auf dem Firmenserver wird der Datenschutzbeauftragte also nicht mehr zurecht kommen. Darauf weisen auch die bayerischen Datenschutzaufseher Kranich und Sachs in ihrem Buch ausdrücklich hin. Gefragt ist ein Datenschutz-Managementtool, das alle direkten und indirekten Dokumentations-Anforderungen der Verordnung abbildet, und dennoch einfach zu bedienen ist. »Es reicht ja nicht mehr, wenn sich nur der Datenschutzverantwortliche auskennt, auch das macht unser kleines Beispiel klar«, gibt Volkmer zu bedenken.

Einfacher Umstieg auf Privacysoft

Datenschutz-Tool von Projekt 29 bietet Migrationssupport für alle gängigen Software-Lösungen

Die Uhr tickt. Nur noch ein paar Monate, bis im Mai 2018 die Regelungen der EU-Datenschutzgrundverordnung (DS-GVO) einzuhalten sind. Experten sind sich einig, dass es ohne ein professionelles Datenschutz-Managementtool wohl kaum möglich sein wird, die komplexen Anforderungen zu erfüllen. Privacysoft, die Datenschutz-Software von Projekt 29, ist schon jetzt optimal auf die DS-GVO vorbereitet. Das System bietet Schnittstellen zum schnellen und einfachen Umstieg aus den meisten anderen Lösungen.

Durch die neue EU-Verordnung ist das Datenschutzrecht im Umbruch. Erst nach und nach kristallisieren sich die Vorstellungen der Aufsichtsbehörden zur korrekten Umsetzung der Paragraphen heraus. Noch über viele Jahre werden Rechtsstreitigkeiten und Gerichtsurteile immer wieder Neu- und Nachjustierungen für die Praxis bringen. Privacysoft ist deswegen von vornherein nicht als fertiges Softwarepaket zur einmaligen

Installation angelegt, sondern als Online-Lösung, die laufend aktualisiert wird. Ändern sich die Vorgaben, findet der Anwender kurzfristig angepasste Vorlagen und Arbeitsabläufe im System. Zu vertretbaren monatlichen Mietkosten bleiben Abonnenten stets auf Höhe der Zeit.

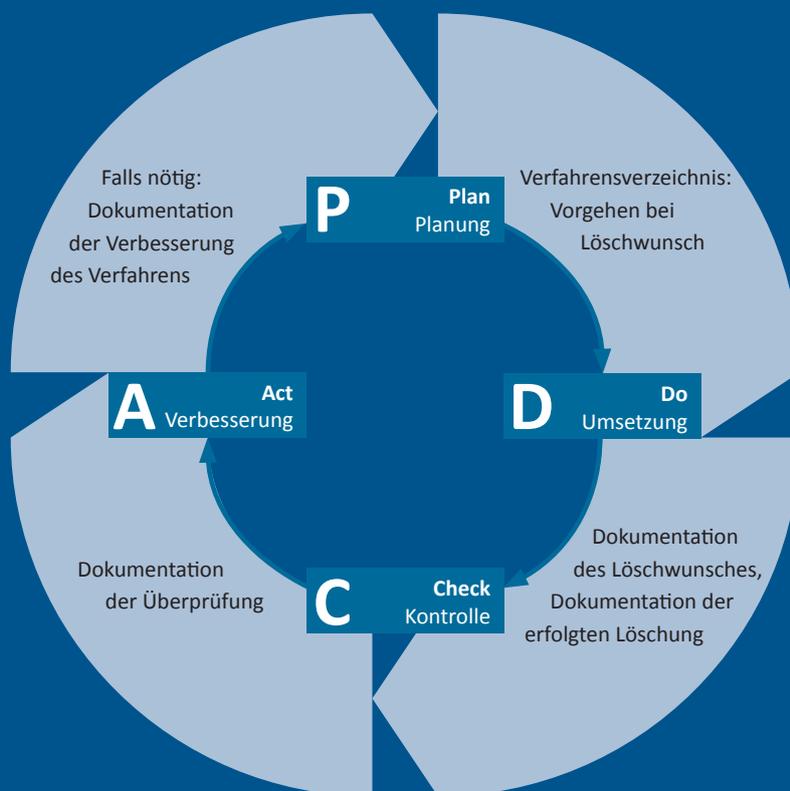
»Wer aus klassischen Lösungen in das modernere System wechseln möchte, muss nicht bei null anfangen«, sagt Privacysoft-Produktmanager Manfred Gerber. Über eigens angepasste Schnittstellen lässt sich der oft über Jahre aufgebaute und gepflegte Datenbestand importieren. »Damit wird der Umstieg aus zum Beispiel DPRREG, BDSGBasics oder dsbAssist zum Kinderspiel«, verspricht Gerber. Projekt 29 hat nicht nur Importschnittstellen eingebaut, sondern liefert auch mit detaillierten Anleitungen den nötigen Migrationssupport, damit die Vorbereitung auf alle kommenden Anforderungen durch die DS-GVO reibungslos klappt.

Weitere Informationen:

www.privacysoft.de

 **Projekt 29**

An vorderster Front gefordert ist der Callcenter-Mitarbeiter, der das Löschersuchen seines Anrufers vermerken muss. Dann muss der Vorgang in der Kundenbetreuung auflaufen und umgesetzt werden. Der Datenschutzbeauftragte muss all diese Schritte nachvollziehen können. Im Hintergrund sollte das Datenschutztool die Vorgänge protokollieren und revisionssicher abspeichern, so dass der Verantwortliche jederzeit gerüstet ist, wenn die Aufsichtsbehörde zur Überprüfung anrückt.



PDCA-Zyklus am Beispiel des Löschersuchens eines Kunden. Die DSGVO verlangt die lückenlose Dokumentation entlang einer ständigen Kontrolle und Verbesserung des Datenschutzes.

Spezialsoftware für Datenschutzmanagement

»Unternehmen, Verbände, Freiberufler und deren Datenschutzbeauftragte brauchen Werkzeuge, die ihnen die Arbeit abnehmen«, sagt Volkmer. Darin hat Projekt 29 langjährig Erfahrung. Volkmer und seine Mitarbeiter halten aktuell bundesweit über 2.500 Mandate als externe Datenschutzbeauftragte in Organisationen aller Größen.

Aus dieser Marktkenntnis heraus hat das Unternehmen eine eigene Software für das Datenschutzmanagement entwickelt. Das Produkt Privacysoft integriert bereits jetzt die Vorschriften der kommenden DS-GVO.

Das Lizenzsystem von Privacysoft ist darauf ausgerichtet, dass sich künftig viele verschiedenen Mitarbeiter mit Datenschutzthemen befassen müssen. Es reicht, pro Unternehmen eine Lizenz zu erwerben, egal wie viele Mitarbeiter das Produkt benutzen. Als Online-System lässt sich Privacysoft ohne Installation von jedem Computer aus aufrufen.

Privacysoft zeigt nur die Funktionen, die jeweils benötigt werden. So erfasst der Callcenter-Mitarbeiter mit wenigen Klicks das Löschersuchen, die Kundenbetreuung bestätigt mit wenigen Klicks die Umsetzung. Erst dem Datenschutzbeauftragten ist das komplette System zugänglich, das ihn bei den komplexen täglichen Aufgaben leitet und unterstützt.

Besonders nützlich ist für die Praxis, dass alle Updates im Monatspreis enthalten sind. »Sobald neue Vorschriften und Ausführungsbestimmungen bekannt werden, setzen wir sie in Privacysoft um. Wer das Produkt nutzt, ist immer auf Höhe der Zeit«, so Christian Volkmer.

Mit Privacysoft entspannt zurücklehnen

Das Allround-Werkzeug für alle Datenschutzaufgaben

Datenschutz und korrektes Datenschutzmanagement sind schon jetzt Mammutaufgaben. Die kommende EU-Datenschutz-Grundverordnung (DS-GVO) sattelt noch einmal drauf. Auf Unternehmen und Organisationen kommen deutlich mehr Pflichten zu. Die Bußgelder steigen bis in den achtstelligen Bereich. Die Regensburger Projekt 29 GmbH & Co. KG stellt just zu diesem Zeitpunkt mit Privacysoft eine völlig neue Software zum Datenschutzmanagement vor. Für die DS-GVO ist das Produkt bestens präpariert.

„Wir halten über 2.500 Mandate als externe Datenschutzbeauftragte“, sagt Christian Volkmer, Inhaber von Projekt 29. In ganz Deutschland betreut und berät sein Unternehmen Verbände, Vereine, Arztpraxen und Kammern sowie Firmen von 10 bis 36.000 Mitarbeitern. Das, gepaart mit seinem Know-how als Informatiker und den Erfahrungen, die er ab 1996 mit seinem eigenen IT-Systemhaus machte, „hat quasi ganz automatisch zu einer eigenen Software-Plattform für das Datenschutzmanagement geführt“, so Volkmer. „Zusätzlich angetrieben hat uns, dass wir am Markt keine Lösung gefunden haben, mit der wir für unser Geschäft als externe Datenschutzbeauftragte zufrieden gewesen wären.“

Privacysoft hat Antworten auf alle Erfordernisse, mit denen Projekt 29 tagtäglich konfrontiert ist. Äußerst flexibel unterstützt und erleichtert die Softwareplattform die Arbeit von Verantwortlichen für den Datenschutz bei allen gültigen gesetzlichen Bestimmungen. Die kommenden Anforderungen der DS-GVO sind schon berücksichtigt. „Selbstverständlich fließen Änderungen in Gesetz und Rechtsprechung über Updates unmittelbar in die Software ein“, erläutert Volkmer.

Den Benutzer empfängt eine zeitgemäße, intuitive und leicht bedienbare Benutzeroberfläche, die alle Funktionen übersichtlich strukturiert.

Wie bei modernen Websites passt sich das responsive Design automatisch der Bildschirmgröße vom Smartphone bis zum Desktop-PC an. Ein integrierter Assistent (Wizard) führt die Anwender durch Workflows. Aktuelle Checklisten, Musterverfahren und Vorlagen helfen, die Unternehmensprozesse zu beleuchten und zu bewerten.

Rechtssichere Dokumentation und umfangreiche Reports

Wirkungsvoll und zeitsparend entsteht bei der Erfassung, Kontrolle, Steuerung, Analyse und Optimierung der Arbeitsabläufe aller Datenschutzprozesse quasi nebenbei eine revisions-sichere Dokumentation der vorhandenen Verfahren und Maßnahmen. Umfangreiche Reportfunktionen und der Im- und Export von Daten in gebräuchlichen Dateiformaten gehören zum Ausstattungsumfang. Die Multimandantenfähigkeit macht es möglich, beliebige betriebliche oder konzernweite Strukturen darzustellen und zu verwalten.

Auch das Thema Auftragsdatenverarbeitung

(ADV) lässt sich komfortabel abbilden. Neben der Verwaltung von ADV-Verträgen können mit Privacysoft auch die technischen und organisatorischen Maßnahmen (TOM) von externen Dienstleistern systematisch geprüft und dokumentiert werden.

„Nicht nur gesetzliche Vorschrift sondern ein echtes Anliegen ist uns die Schulung und Sensibilisierung von Mitarbeitern“, betont Christian Volkmer. Deswegen beinhaltet Privacysoft eine optionale Funktion, um in Unternehmen flächendeckend Online-Schulungen, Webtrainings und Webcasts bereitzustellen. Alle Schulungsinhalte erfüllen die Anforderungen des Bundesdatenschutzgesetzes (§ 5 BDSG) und der DS-GVO. Höchst flexibel gestaltet sich die Nutzung von Privacysoft. Die Software steht als in Deutschland gehostete Cloud-Lösung zur Verfügung, die aktuelle Webbrowser und mobile Endgeräte wie Smartphones und Tablets unterstützt. Das Rechenzentrum ist nach ISO 27001 zertifiziert.

Weitere Informationen und Demoterminevereinbarung unter www.privacysoft.de

NEU!

PRIVACYSOFT

Die modulare Software-Plattform für alle Aufgaben im Datenschutzmanagement.

► Jetzt Online-Präsentation vereinbaren!

Unter Tel. 0941 2986930 erwartet Sie ein freundlicher Ansprechpartner.

WAS DER DATENSCHUTZ VON DER INFORMATIONSSICHERHEIT LERNEN KANN – VOM ISMS ZUM DSMS

Andreas Liefeith

In Projekten zur Einführung eines Informationssicherheits-Management-Systems (ISMS) haben wir in den vergangenen Jahren die Erfahrung gemacht, dass der Aufwand für die Dokumentation von vielen Kunden deutlich unterschätzt wurde. Bei einem mittleren Stadtwerk sind es immerhin über 40 Dokumente, die erstellt, und noch wichtiger, de facto über einen unbegrenzten Zeitraum aktuell gehalten werden müssen. Und das bei immer kürzeren Technologizeyklen!

Droht jetzt beim Datenschutz das gleiche Dilemma? Mit großer Wahrscheinlichkeit: JA!

Denn mit Inkrafttreten der DS-GVO ist der Umgang mit personenbezogenen Daten in allen Geschäftsprozessen in sog. Verarbeitungsverzeichnissen zu dokumentieren und es ist davon auszugehen, dass Aufsichtsbehörden dies früher oder später auch überprüfen werden.

Lassen Sie mich an einem Beispiel verdeutlichen, was das für ein mittelständisches Unternehmen, wie procilon bedeutet.

Wir stellen in unterschiedlichem Kontext elektronische Zertifikate aus oder sind unseren Kunden bei der Beschaffung behilflich. Da es sich bei solch einem Zertifikat um ein hochwertiges digitales Objekt handelt, das unter Umständen die eigenhändige Unterschrift ersetzt, schreibt der Gesetzgeber eine geeignete aber auf jeden Fall eine eindeutige Identifikation vor. Der Identifikationsprozess erhebt, je nach gewünschtem Zertifikat, unterschiedliche personenbezogene Daten, die von Vorname, Name, Anschrift etc. bis hin zu einer Ausweiskopie gehen können.

Aus Sicht des Datenschutzes muss sich also procilon Gedanken machen, wie man damit umgeht. Erschwerend kommt dazu, dass diese Überlassung

auch noch analog (Brief) oder digital (E-Mail) erfolgen kann. Und da man diese Daten auch nur für den Zeitraum der Geschäftsbeziehung, also in unserem Beispiel der Gültigkeitsdauer des Zertifikats, üblich sind 2-3 Jahre, speichern darf, tickt nebenbei auch noch eine Aufbewahrungsfrist.

Um sicherzustellen, dass wir den Regeln des Datenschutzes entsprechend handeln, war es also notwendig technische und organisatorische Maßnahmen – nennen wir sie TOMs – zu ergreifen. Dazu gibt es in der einschlägigen Gesetzgebung ausreichend Lesestoff und wir wollen hier exemplarisch einmal drei daraus abgeleitete Fragestellungen herausgreifen:

- Wo werden personenbezogene Daten gespeichert?
- Wie werden personenbezogene Daten geschützt?
- Wer hat Zugriff auf diese Daten?

Und spätestens an dieser Stelle müssen alle, die sich mit Informationssicherheit, ISMS und Co. schon einmal beschäftigt haben, sicher stutzen.

Ja, richtig! Wenn man auf Basis einer Risikobewertung für Kunden-, Lieferanten- oder Mitarbeiterdaten zu dem richtigen Ergebnis »Schutzbedarf hoch« gekommen ist, müssten die drei Fragen durch einen Blick in die Dokumente des ISMS schnell zu beantworten sein.



Hier laufen gleich mehrere Handlungsstränge zusammen, denn in der DS-GVO sind Verarbeitungsverzeichnis und Vorabkontrolle neu geregelt und

gleichen einem Risikomanagement wie ein Ei dem anderen. Die EU hat mit der DS-GVO die bisherigen Vorgaben deutlich erweitert. Damit wird aus einem punktuellen Datenschutzkonzept ein kontinuierlicher Managementprozess, der auch eine ständige Risikoanalyse beinhaltet und analog zum ISMS-Zyklus abgebildet werden kann.

In nicht zu weit entfernter Zukunft wird mit Inkrafttreten der EU-Datenschutzgrundverordnung, grade unter Berücksichtigung möglicher Sanktionen, der Dokumentationspflicht im Datenschutz im Sinne von entsprechenden Verarbeitungsverzeichnissen größte Wichtigkeit zugemessen. Prinzipiell gelten hier die gleichen Anforderungen an das Änderungsmanagement der zugehörigen Dokumente wie bei

der Informationssicherheit. Also liegt der Einsatz von entsprechenden Werkzeugen auch dafür nahe. Doch damit nicht genug. Wegen der hohen Flexibilität solcher Werkzeuge kann ein Einsatz in den Bereichen Gefahrstoff-, Fuhrpark-, Gebäude- und Lizenzmanagement auch sehr intensiv betrachtet werden. Synergien zur Herstellung von Compliance solch innovativer Vorhaben sind de facto keine Grenzen gesetzt.



Der Datenschutz wird eine neue Qualität gehoben.

Kommen wir aber erst einmal zurück zu unserem Verarbeitungsverzeichnis. Wenn also Daten, die man dafür braucht, schon im ISMS vorhanden sind, kann mal diese natürlich auch zu dessen Erzeugung heranziehen. Der Aufwand zur Dokumentation der TOMs verringert sich erheblich und die Aktualität ist gegeben, wenn man es richtig macht.

Die eingangs geschilderten Projekterfahrungen aus dem KRITIS-Bereich haben gezeigt, dass der Dokumentationsaufwand nur mit IT-Unterstützung, also einem intelligenten Werkzeug, zu bewältigen ist. Solche Werkzeuge sind heute meist schon bei der Unterstützung von IT-Service-Management-Prozessen zur Dokumentation von Vorgängen und Assets im Einsatz. Aktuell werden diese oft um die Möglichkeit der Abbildung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 erweitert oder separat für diesen Zweck eingeführt.

Damit ist der Schritt zum kontinuierlichen Datenschutz-Managementsystem (DSMS) vollzogen.

Das ISMS wird um die Komponente DSMS ergänzt!

Über den Autor

Andreas Liefeith

Leiter Marketing und Partnermanagement
procilon GROUP



► www.procilon.de



WAS STECKT HINTER DER VERSIEGELTEN CLOUD DER TELEKOM?

Dr. Hubert Jäger, CTO Unicon GmbH

Ende März 2017 hat die Deutsche Telekom ihre Magenta Security Services um das Angebot der »Versiegelten Cloud« erweitert. Der Dienst soll selbst für Träger von Berufsgeheimnissen, wie etwa Ärzte, Anwälte und Behörden, geeignet sein. Doch was steckt dahinter? Welche Technologie unterscheidet die Versiegelte Cloud von anderen Cloud-Services?

Datenschutz und Vernetzung – zwei Schlagwörter, die die Digitalisierungs-Diskussionen von Unternehmen und Politikern dominieren. Die einen fordern mehr Schutz für die Daten der Bürger, die anderen geben gerade den strengen Datenschutzgesetzen und Compliance-Regeln in Deutschland die Schuld an dem als zu langsam empfundenen digitalen Wandel. Tatsache ist jedoch: IT-Sicherheit und der Schutz unternehmenseigener Daten sind Grundvoraussetzungen dafür, dass sich verantwortungsbewusste Unternehmen dem Digitalisierungsprozess überhaupt anschließen können.

Grundsätzlich gibt es im Cloud-Computing drei große potenzielle Cloud-Sicherheitslücken, die es zu bedenken gibt: Den unberechtigten Zugriff durch Dritte während des Datentransfers zwischen Endgerät und Cloud, den Zugriff in der Datenbank bzw. im Storage-System und den unbefugten Zugriff durch den Dienstbetreiber oder seine Mitarbeiter während der Verarbeitung der Daten in den Prozessoren der Server. Zwei dieser drei Sicherheitslücken – der Zugriff während des Transfers und der Zugriff im Storage-System – gelten gemeinhin als gelöst. Die Ansätze, das dritte Problem – den Betreiberzugriff – in den Griff zu kriegen, waren bisher kompliziert und aufwändig und galten als nur bedingt vertrauenswürdig.

Was also ist bei der Versiegelten Cloud anders?

Schafft Münchner Technologie Datensicherheit?

Hinter der versiegelten Cloud der Telekom steckt die international patentierte Sealed Cloud Technologie des Münchner High-Tech-Unternehmens und Cloud-Sicherheits-Spezialisten Unicon. Grundaufgabe bei der Entwicklung dieser Basistechnologie war es, mit rein technischen Mitteln sicherzustellen, dass die Übertragung und

Speicherung von Daten verschlüsselt erfolgt und dass Daten – Inhalte wie Verbindungsinformationen – auch während der eigentlichen Verarbeitung geschützt sind. Wo andere Cloud-Service-Anbieter organisatorische und technische Maßnahmen kombinieren, um die Daten in der Cloud zu schützen, wählt die Sealed Cloud einen anderen Ansatz: Indem sie organisatorische Maßnahmen durch technische ersetzt, will sie den Unsicherheitsfaktor Mensch umgehen. Doch wie genau funktioniert das?

Für den Schutz beim Transport zum und vom Datenzentrum sorgt eine Verschlüsselung, beispielsweise eine klassische SSL-Verschlüsselung, allerdings mit einer Beschränkung auf sichere Verfahren – d.h. es werden nur Cipher verwendet, von denen keine Sicherheitslücke bekannt ist, deren Schlüssel lang genug gewählt sind und die den Betreiber durch »perfect forward secrecy« ausschließen.

Die Daten in der Datenbank bzw. im Storage-System sind ebenfalls verschlüsselt. Gängige technische Lösungen verschlüsseln die Daten in der Datenbank bzw. im Storage-System auf Block-Ebene mit einem oder einer geringen Zahl systemweit gültiger Schlüssel, die dann im Schlüsselspeicher aufbewahrt werden. Die Versiegelte Cloud geht hier weiter: Ein spezieller Algorithmus generiert während des Anmeldevorgangs aus den Login-Informationen (Username, Passwort und gegebenenfalls weiteren Daten) einen individuellen Schlüssel für jeden einzelnen Nutzer. Dieser findet die Daten des Anwenders, entschlüsselt sie und lädt sie in den Hauptspeicher.

Nach dem Abmelden verschlüsselt und speichert das System die Daten erneut und zerstört den zuvor generierten nutzerindividuellen Schlüssel. In der Datenbank mit einer bestimmten Anzahl von Nutzern existieren somit ebenso viele verschiedene Nutzerdatensätze, die jeweils individuell nach AES256 (Advanced Encryption Standard: symmetrisches Verschlüsselungsverfahren mit einer Schlüs-



Dr. Hubert Jäger,
CTO Unicon GmbH

sellänge von 256 Bit) verschlüsselt sind. Da die Schlüssel nicht im System abgelegt sind, ist die Zugangshürde für interne und externe Angreifer außerordentlich hoch. Ein Angreifer müsste also den AES256 knacken, und dies jeweils separat für jeden Nutzerdatensatz bzw. jede Datei.

Betreiberzugriff technisch ausgeschlossen

Damit verbleibt zuletzt noch der Hauptspeicher der Server als potentielles Ziel für Insider-Angriffe. Denn hier liegen die Daten während einer aktiven Session wie überall in Klarschrift, also unverschlüsselt, vor. Ein Administrator könnte beispielsweise einen sogenannten Memory Dump ziehen und diesen zu einem passenden Zeitpunkt in aller Ruhe auswerten. Im System der Versiegelten Cloud sollen deshalb ein »Data-Clean-Up« genanntes System und eine ganze Reihe zusätzlicher Maßnahmen die Server vor Zugriffen schützen.

Bei einem Data-Clean-Up geschieht Folgendes: Alle Applikationsserver befinden sich in elektromechanisch versiegelten Rack-Systemen. Darüber hinaus beinhalten die Server nur flüchtige Speicher, die sich nach Stromabschaltung von selbst leeren. Das verwendete Betriebssystem ist zusätzlich gehärtet und sperrt die externen Zugänge. Außerdem meldet das System zwar Statusinformationen nach außen, akzeptiert jedoch keine administrativen Anweisungen oder anderweitige Befehle aus der Ferne. Für jegliche Administration muss man also das jeweilige Segment eines Serverschranks manuell öffnen.

Dazu erhält der Betreiber nur Zugang, wenn der Kunde ihm einen Arbeitsauftrag und einmaligen Zugangscode gibt. Bevor sich das Rack-System öffnen lässt, werden alle Daten auf andere sichere Server verschoben und der Server heruntergefahren und für zehn Sekunden stromlos gestellt. Arbeitet also der Administrator zur Wartung am System, ist dieses vollkommen frei von Anwendungsdaten.

Auf diese Weise soll ein Zugriff Unberechtigter komplett ausgeschlossen werden.

Die Kombination der beschriebenen Maßnahmen soll sicherstellen, dass im Datenzentrum kein Zugriff auf unverschlüsselte Daten erfolgen kann – auch nicht durch den Betreiber des Cloud-Dienstes oder seine Mitarbeiter.

Schutz der Metadaten

Ein weiteres Element, dass bei der Sealed-Cloud-Technologie zum Tragen kommt, ist der Schutz der Verbindungsdaten von den Nutzern (Metadaten). Der Grund für diese Maßnahme: Metadaten sagen viel über die Absichten der betroffenen Parteien aus und sind einfach zu analysieren. Ein adäquater Datenschutz und die Informations-Sicherheit müssen auch den Schutz dieser Metadaten miteinschließen.

Damit keine Rückschlüsse auf Metadaten gezogen werden können, indem Außenstehende das Verkehrsaufkommen beobachten, werden die Benachrichtigungen über den Verkehr zufällig zeitverzögert. ▶

Datenschutz bei Datenaustausch und Zusammenarbeit

Anforderungen der datenschutzkonformen Organisation



Stand der Technik
"Sealed Cloud Betreibersicherheit"



**VERSIEGELTE
CLOUD**



Rechtswirkung



Zukunftssicher dank »Privacy by Design«

Die im nächsten Jahr in Kraft tretende europäische Datenschutz-Grundverordnung (EU-DSGVO) fordert in Artikel 25 »Datenschutz durch Technikgestaltung«. Damit gilt der Stand der Technik neben den Implementierungskosten als Maßstab dafür, was als angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten angesehen wird.

Dank ihres Konzepts, schon bei der Entwicklung Datenschutz mit zu berücksichtigen (»Privacy by Design«), entspricht die Sealed-Cloud-Technologie diesen Anforderungen. Uniscons eigener Cloud-Dienst beispielsweise hat dank der zugrundeliegenden Basistechnologie als einer der ersten deutschen Dienste das Datenschutz-Zertifikat nach dem Trusted Cloud Datenschutzprofil (TCDP) in der höchsten Schutzklasse erhalten. Das TCDP ist ein Prüfstandard für die Datenschutz-Zertifizierung von Cloud-Diensten und baut auf dem ISO/IEC-Standard 27018 auf, der wiederum die international anerkannten ISO/IEC-Standards 27001 und 27002 um Cloud- und datenschutzspezifische Anforderungen er-

weitert. Weil der Dienst in Schutzklasse III zertifiziert ist, ist er nicht nur für Träger von Berufsgeheimnissen nach § 203 StGB geeignet, sondern befreit den Anwender auch von seiner Kontrollpflicht nach § 11 Absatz 2 BDSG.

Die EU-DSGVO konstituiert Datenschutz durch Technikgestaltung. Cloud-Angebote halten die Implementierungskosten niedrig. Schaffen es Angebote beides zu kombinieren, dürfte es Unternehmen künftig nicht mehr schwerfallen, Datenschutz dem Stand der Technik entsprechend umzusetzen.

Über den Autor



Dr. Hubert Jäger

Gründer und CTO bei Uniscon sowie stellv. Vorsitzender des AK Cloud Computing & Outsourcing beim Digitalverband Bitkom

► www.uniscon.de



Dienste mit Sealed-Cloud-Technologie

Derzeit gibt es in Deutschland drei verschiedene Cloud-Dienste, die auf der Sealed-Cloud-Technologie basieren:

- **iDGARD (Uniscon GmbH)**

Cloud-Dienst aus Deutschland für digitalen Datenaustausch und virtuelle Datenräume (<https://www.idgard.de/>)

- **uCloud (regio iT)**

Dokumente zentral verwalten und teilen mit dem persönlichen und mobilen Datenspeicher der regio iT. (<http://ucloud.regioit.de/home/home.html>)

- **Die Versiegelte Cloud (Deutsche Telekom/Magenta Security)**

Der Cloud-Speicher mit der höchsten Sicherheit im Rechenzentrum der Deutschen Telekom. (<https://cloud.telekom.de/magenta-security/versiegelte-cloud/>)

WEITERFÜHRENDE LITERATUR:

- Trusted Cloud Datenschutzprofil: <http://www.tcdp.de/data/pdf/TCDP-1-o.pdf>
- Schutzklassen in der Datenschutz-Zertifizierung: Steffen Kroschwald, Informationelle Selbstbestimmung in der Cloud: datenschutzrechtliche Bewertung und Gestaltung des Cloud Computing aus dem Blickwinkel des Mittelstands. In: DuD Fachbeiträge Wiesbaden 2016.
- Hubert Jäger et al, A Novel Set of Measures Against Insider Attacks. In: Detlev Hühnlein & Alexander Roßnagel (Hrsg.), Proceeding of Open Identity Summit 2013. Lecture Notes in Informatics (BD. 223).

Seminare und Lehrgänge.

Für eine gesetzeskonforme und professionelle Umsetzung von Datenschutz und Compliance.



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

Datenschutz

- Datenschutzfachkraft
- Datenschutzbeauftragter (TÜV)
- Datenschutzauditor (TÜV)
- Externer Datenschutzbeauftragter (TÜV)
- Datenschutz-Update
- EU-Datenschutz-Grundverordnung

Weitere Infos und Anmeldung unter:
www.tuv.com/datenschutz

Weitere Informationen erhalten Sie 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

Compliance

- Compliance Officer (TÜV)
- Compliance-Beauftragter
- Korruptionsprävention
- Compliance-Organisation
- Compliance-Risikoanalyse
- Interne Untersuchungen

Weitere Infos und Anmeldung unter:
www.tuv.com/compliance

SENSIBILISIERUNG ZUM THEMA »SOZIALE MANIPULATION«

Stefan Bachmann, INES IT



Organisatorische IT-Sicherheit spielt gerade in Bezug auf Ransomware oder Geschäftsführerbetrug eine immer entscheidendere Rolle. Allen Angriffsvarianten ist dabei wohl eines gemeinsam, sie beinhalten soziale Manipulation (Social Engineering). Nur durch vorhersehbares Handeln der Opfer führt ein Angriff zum Erfolg.

Wir als Datenschutzbeauftragte können hier eine wichtige Aufgabe im Unternehmen umsetzen, die Sensibilisierung der Mitarbeiter explizit zu diesen Themen.

Das Wort »explizit« wurde bewusst gewählt, denn meist gestalten wir unser Schulungsprogramm mit weiteren Schwerpunktthemen wie Zutritts-, Zugangs- oder Weitergabekontrolle aus. Für eine tiefgehende Auseinandersetzung mit den Grundsätzen der Angriffsszenarien bleibt meist keine Zeit.

Im Zuge eines Kundenschulungsprogramms Mitte Mai 2017 machte ich für mich die positive Erfahrung, dass eine umfassende Aufklärung zu »sozialer Manipulation« einen tollen Erfolg brachte. Man spürte förmlich, dass die vorab vermittelten Grundsätze den nachfolgenden praktischen Fallbeispielen gegenübergestellt und das mögliche Risiko für das Arbeitsumfeld erkannt wurde.

Soziale Manipulation – was ist das überhaupt?

In der IT-Sicherheit versteht man darunter die Manipulation von Menschen mit dem Ziel, unwillentlich und unwissentlich eine bestimmte Handlung auszuführen. Dies kann beispielsweise die Weitergabe sensibler Informationen, das Anstecken eines USB-Sticks oder das Öffnen eines E-Mail Anhangs sein.

Wieso funktioniert Soziale Manipulation?

Menschen besitzen Verhaltensregeln, die in der Evolution entstanden und uns fest einprogrammiert sind, sogenannte Fixed Action Pattern (FAPs). Ein Beispiel dafür wäre Konsistenz, eine zentrale Verhaltensgrundlage von Menschen: »wenn jemand eine Aussage tätigt tut (ist) er das auch«. Auf Basis dieser Maxime leben Gesellschaften, weil ohne konsistentes Verhalten Prozesse nicht funktionieren könnten.

FAPs werden seit geraumer Zeit von Verhaltensbiologen untersucht und an Hand von Experimenten nachgewiesen, wie dieser Versuch von M.W. Fox aus dem Jahr 1974.

In ein Truthahngelege wurde ein ausgestopftes Wiesel, ein natürlicher Feind des Truthahns, gelegt. Im Kopf der Truthahnhenne wurde die FAP ausgelöst: Feind im Gelege sofort attackieren. Die Truthahnhenne ging auf das Wiesel los.

Im Körper des Wiesels war ein Lautsprecher installiert. Nun ließen die Forscher über diesen Lautsprecher die Laute von Truthahnküken abspielen.

In der Truthahnhenne wurde eine neue FAP abgerufen: Wenn Truthahnküken, dann bemuttern. Die Henne blendete alle sichtbaren Hinweise aus und fing an das Wiesel zu bemuttern.¹

Social Engineering greift genau diese Grundprinzipien in uns an, wie folgendes Beispiel auf tragische Weise zeigt:

Der Flugzeugzulieferer FACC aus Ried im Innkreis Oberösterreich verlor durch Soziale Manipulation 50 Millionen Euro. Vierzig gefälschte E-Mails vom Vorstandsvorsitzenden reichten aus, das notwendige Vertrauen aufzubauen. Der betroffene Mitarbeiter verhielt sich konsistent und ging von einem realen, vertraulichen Geschäftsvorgang aus.

Praktische Beispiele

Betroffene betroffen machen ist ein Zitat von Stefan Purder, dass die »praktische« Schulungsphase treffend beschreibt. In meinem Vortrag habe ich neben anderen Beispielen eine gefälschte E-Mail des IT-Leiters an einen externen Spezialisten für Forensik gezeigt.

Darin wurde beschrieben, dass ein massives Sicherheitsproblem im Firmennetzwerk vorliege. Eine interne Manipulation kann nicht ausgeschlossen werden. Der externe Forensiker

wurde beauftragt nach seiner empfohlenen Vorgehensweise den Fall aufzuarbeiten. Auch der telefonischen Abfrage von Login Daten ausgewählter Mitarbeiter wurde stattgegeben. Als Legitimation sollte die E-Mail beim Telefongespräch an den jeweiligen Mitarbeiter zugestellt werden.

Absolute Verschwiegenheit auch gegenüber Kollegen wurde angeordnet, da eine interne Manipulation nicht ausgeschlossen werden könne.

Gefühlt einhundert Prozent der Teilnehmer wären auf diese Phishing-E-Mail hereingefallen und Betroffenheit war in den Gesichtern zu lesen.

Ansprechpartner und Lösungsansätze

Natürlich dürfen die Mitarbeiter an dieser Stelle nicht alleine gelassen werden. Hier sind Lösungsansätze das geeignete Mittel die Betroffenheit in Effektivität für die Unternehmenssicherheit zu wandeln. Stellen Sie diese Lösungsansätze zentral zu Verfügung. Am besten, Sie geben diese parallel im Vortrag in Papierform aus. Damit ist ein schneller Zugriff auch ohne IT gegeben.

Unbedingt notwendig für die Mitarbeiter sind erreichbare, vertrauensvolle Ansprechpartner. An diese können ungewöhnliche Vorgänge gemeldet und mögliche Fehler offenbart werden.

Fazit

Für mich war dieses Schulungskonzept ein deutlicher Mehrwert bei der Sensibilisierungsarbeit. Dies spiegelte sich auch in dem Feedback der Teilnehmer und Organisatoren wieder. Ich kann Sie nur ermuntern dieses Schema ebenfalls zu versuchen.

Ihr Stefan Bachmann

Über den Autor

Stefan Bachmann

ist seit 26 Jahren bei der INES IT in Unterneukirchen beschäftigt; seit 2009 wirkte er am Aufbau der Abteilung Datenschutz und IT-Sicherheit mit. Heute bietet die INES IT in diesem Bereich Datenschutz- und IT-Sicherheitsberatung, Securityaudits sowie Penetrationstests.

► www.ines-it.de



► INES IT

¹ Stefan Schumacher – Die psychologischen Grundlagen des Social Engineerings (CCC2011)

FRAGEBOGEN FÜR KÜNFTIGE UNTERNEHMENSPRÜFUNG NACH DS-GVO

Das Bayerische Landesamt für Datenschutzaufsicht hat für Unternehmen zur Vorbereitung auf den Start der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 einen Fragebogen veröffentlicht. Damit will sie dem Management und den Datenschutz-Beauftragten in Firmen eine Vorstellung geben, wie eine künftige Prüfung aussehen könnte.

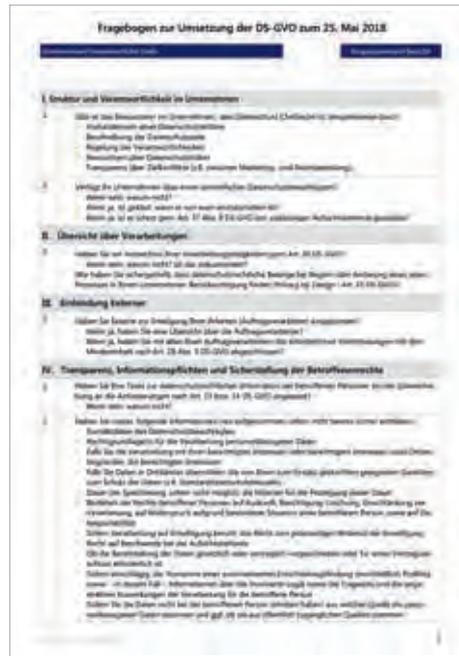
Unter anderem fragt die Aufsichtsbehörde nach Datenschutzleitlinien, Datenschutzbeauftragten und dem Verzeichnis der Verarbeitungstätigkeiten. »Insbesondere die Anforderungen an die Transparenz und Nachweisbarkeit der gesetzeskonformen Datenverarbeitung sind gestiegen und stellen viele Unternehmen vor gewaltige Herausforderungen«, schrieb Landesamts-Präsident Thomas Kranig. Weitere Themen sind unter anderem der Umgang mit Risiken und mit Datenschutzverletzungen

Kranig mahnte, mit der DS-GVO erhalten Bürgerinnen und Bürger klar geregelte Ansprüche beispielsweise auf Auskunft, Berichtigung, Löschung und Einschränkung bei der Verarbeitung ihrer personenbezogenen Daten. Zudem könnten sie künftig Widerspruch zu einer Verarbeitung einlegen. Dem müssten die Unternehmen Rechnung tragen.

Insgesamt bringe das neue Recht gewaltige Änderungen, auch für jene Betriebe, die bereits Datenschutz-Strukturen nach der alten Datenschutz-Richtlinie von 1995 unverändert beibehalten haben, schrieb Kranig.

Zum Test hatte die Behörde 150 zufällig ausgewählte bayerische Unternehmen den Fragebogen vorab zugeschickt. Alle anderen können den Fragebogen, der sich auch gut als Checkliste zur Vorbereitung eignet, auf der Startseite www.lida.bayern.de herunterladen. (chd)

Der Fragebogen ist auch auf Englisch abrufbar.



ERSTMALS LFDI-PREIS FÜR DATA PROTECTION AND TRANSPARENCY VERLIEHEN



Die Stadt Mainz und die Verwaltung der Verbandsgemeinde Pirmasens-Land sind die Preisträger des erstmals verliehenen LfDI-Preises für Data Protection. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI), Prof. Dieter Kugelmann, überreichte die Preise am 20. Juni in Mainz. Schirmherr war der Präsident des rheinland-pfälzischen Landtags, Hendrik Hering. Das LfDI will den Preis künftig jährlich vergeben.

Die beiden Verwaltungen erhielten den Preis für ihre Ansätze zur Datenschutz-Schulung und Information von Mitarbeiterinnen und Mitarbeitern in der Verwaltung. Die Stadtverwaltung der rheinland-pfälzischen Landeshauptstadt sensibilisierte die Angestellten in einer einjährigen Kampagne zum Thema Informationssicherheit. In Kurzinformationen erhielten sie Hinweise zum praktischen Datenschutz. Die Themen reichten vom korrekten Umgang mit Passwörtern und Speicherorten bis hin zum Angriff auf Computersysteme.

Die Verwaltung von Pirmasens-Land gewann den Award für ihre mittlerweile seit fünf Jahren laufenden Datenschutz-Schulungen. Dabei bieten als Multiplikatoren ausgebildete Mitarbeiter halbjährlich interne Schulungen zu Datenschutz und Datensicherheit an. Damit will die Verwaltung nachhaltiges Wissen und Kompetenzen in der Verwaltung beim Datenschutz aufbauen.

In der zweiten Kategorie Transparency gewann ein gemeinsames Projekt mehrerer Landes-

Kommunalverwaltungen zum Aufbau einer Geodateninfrastruktur. Über eine Plattform können andere Verwaltungen auf Daten wie Bodenrichtwerte, Flächennutzungs- und Bebauungspläne oder Luftbilder zugreifen und selbst für ihre Informationsangebote nutzen. Das sei auch für andere Verwaltungen Anreiz, eigene Daten auf der Plattform bereitzustellen, hieß es in der Preisbegründung. (chd)

LfDI stellt Best-Practice-Empfehlungen für Verwaltungen vor

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, Dieter Kugelmann, hat neue Best-Practice-Empfehlungen für Verwaltungen zur Auswahl und Arbeit von geeigneten Datenschutzbeauftragten vorgestellt. Die Empfehlungen sind das Ergebnis eines Projekts zur Stärkung des kommunalen Datenschutzmanagements. Ziel ist es, Kommunen und Verbänden einen Leitfaden an die Hand zu geben, den sie auf die eigene Organisation übertragen können, wie der LfDI mitteilte.

Unter anderem geben die Best-Practice-Empfehlungen Kommunal- und Kreisverwaltungen einen Leitfaden zur Auswahl und Bewertung eines geeigneten Datenschutzbeauftragten an die Hand. Weitere Themen sind Kommunikation und Netzwerkarbeit von Datenschutzbeauftragten sowie Dokumentation der Datenschutz-Tätigkeit für einen nachhaltigen Datenschutz in der Kommunalverwaltung.

Mit Blick auf den Start der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 sagte Kugelmann: »Die Empfehlungen sind eine gute Grundlage für die Kommunalverwaltungen, sich auf die anstehenden Rechtsänderungen vorzubereiten.« Zugleich will er damit zeigen, dass die dafür notwendigen Maßnahmen auch leistbar sind.

Die Beispiele sind in rheinland-pfälzischen Kommunen entstanden, aber bundesweit übertragbar. Interessierte können sich das Papier auf www.datenschutz.rlp.de herunterladen. (chd)



EINE DAME FÜR DEN DATENSCHUTZ



Erstmals lobt der BvD einen Preis für erklärende Filmbeiträge zum Datenschutz aus – den Datenschutz Medienpreis, kurz DAME. Bis zum 1. November 2017 können sich Filmschaffende, Produktionsgesellschaften, Kreative, Verbände, Jugendorganisationen oder Initiativen mit Dokumentationen, Spielfilmen oder Video-Clips um den Preis bewerben. Dabei zählt nicht, wie viel Geld eine Produktion zur Verfügung hat, sondern wie verständlich und anschaulich sie Einzelaspekte aus dem weiten Feld des Datenschutzes erklärt. Weitere Kriterien sind unter anderem zielgruppengerechte Ansprache und Originalität. Über die Einreichungen entscheidet eine fünfköpfige Jury aus erfahrenen und engagierten Datenschutzexperten. Der Preis selbst wird auf dem BvD-Verbandstag im April nächsten Jahres verliehen.

Die BvD-News stellt die Jury-Mitglieder vor:



Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen

Barbara Thiel ist seit dem 1. Januar 2015 Datenschutzbeauftragte des Landes Niedersachsen und im Jahr 2017 Vorsitzende der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK).

In der DAME-Jury engagiert sich Barbara Thiel, weil sie Datenschutz stärker im Bewusstsein der Öffentlichkeit verankern möchte.

»Der Preis soll Mut machen, sich mit Datenschutz zu beschäftigen, seine Sinnhaftigkeit zu erkennen und aktuellen Fragen auf den Grund zu gehen«, sagt sie.

Das ist aus Sicht Thiels dringend nötig. Denn Datenschutz hat ihrer Einschätzung nach aktuell ein Image-Problem.

»Datenschutz gilt bei vielen als Spielverderber der Digitalisierung, als Verhinderer ohne Fun-Faktor.« Dabei sei das Gegenteil der Fall. »Datenschutz ist kein Hindernis für die Digitalisierung, sondern wesentliche Voraussetzung für deren Gelingen«, sagt sie.

In der Bevölkerung beobachtet sie zudem eine »digitale Sorglosigkeit«, der sie mit Aufklärung und Engagement entgegenwirken möchte. »Denn Datenschutz ist Grundrechtsschutz. Datenschutz sichert die Privatsphäre in einer sich weiterhin schnell verändernden Welt und schafft auf diese Weise gleichzeitig Vertrauen.«

Dabei sieht Thiel auch den Staat in der Pflicht. Gerade im Zuge aktueller oder geplanter Anti-Terror-Maßnahmen müsste die Bundesregierung die Maß-

nahmen transparent machen und klar benennen, zu welchem Zweck welche Daten wie erfasst würden. Das gelte unter anderem für die Videoüberwachung mit biometrischer Gesichtserkennung. »Sie kann die Freiheit, sich in der Öffentlichkeit anonym zu bewegen, gänzlich zerstören«, warnte Thiel. In Kombination mit einem jetzt für die Sicherheitsdienste erlaubten Zugriff auf Passfotos sei es in Zukunft möglich, jede einzelne Person im öffentlichen Raum zu kontrollieren und auf diese Weise die gesamte Bevölkerung videogestützt zu rastern.

Die Aufklärung des Einzelnen über die Risiken der Digitalisierung und die Gefahren für das Grundrecht auf informationelle Selbstbestimmung sei deshalb von elementarer Bedeutung. Hier setzt die ab Mai nächsten Jahres geltende europäische Datenschutz-Grundverordnung an, die den Datenschutzaufsichtsbehörden Aufklärung und Sensibilisierung ausdrücklich als Aufgabe zuweist.

»Aufklärung ist eine Herkulesaufgabe, die letztlich auch von Politik und Gesellschaft geleistet werden muss«, sagt Thiel.

Auch das Entwickeln von Medienkompetenz bei Kindern und Jugendlichen und deren Umgang mit persönlichen Daten beispielsweise in den sozialen Netzwerken ist für die Datenschutzexpertin eine gesamtgesellschaftliche Aufgabe. Zwar kämen junge Menschen als »digital natives« mit den Geräten in technischer Hinsicht spielend zurecht.

»Ich bezweifle aber, dass sie genau wissen, was mit ihren Daten bei der Nutzung passiert.«

Thiel tritt deshalb für eine entsprechende Bewusstseinsbildung bei Kindern ab der fünften Klasse ein.



Frederick Richter, Vorstand der Stiftung Datenschutz

Frederick Richter steht seit vier Jahren an der Spitze der Stiftung Datenschutz. Sofort sagte er zu, als er die Anfrage von BvD-Vorstand Thomas Spaeing erhielt, in die DAME-Jury zu gehen.

Richter liegt Aufklärung beim Datenschutz am Herzen, weil er darin die Grundlage für eine freie Entscheidung der Bürgerinnen und Bürger sieht. Dafür sei auch Transparenz wichtig, sagt er. Allerdings sieht er die Menschen auch in der Pflicht.

»Der Gesetzgeber kann den Bürgerinnen und Bürgern die Aufgabe, die eigenen Daten zu schützen, nicht vollständig abnehmen. Ohne einen gewissen Aufwand wird die Entscheidungsfreiheit nicht zu erhalten sein«, sagt er.

Die Datenschutzerklärung im wahrsten Sinne des Wortes online abzuheften, aber nicht zu lesen, wie es die meisten Verbraucher tun, sei nicht ausreichend.

Argumente, Verbraucher müssten die Datenschutzbestimmungen einzelner Anbieter so oder so akzeptieren, lässt Richter nicht gelten. »Wir können sehr wohl mit den Füßen abstimmen und von jenen Dienstleistern beispielsweise Abstand nehmen, die ihre Datenschutzrichtlinien nicht verständlich erklärten«, sagt er.

Die Stiftung Datenschutz vergibt in diesem Jahr selbst erstmals einen Journalistenpreis, gemeinsam mit der Deutschen Fachpresse. Die Auszeichnung prämiiert ausgewogene Berichte in Print-Medien zu den Risiken und Chancen der digitalen Welt.

Den DAME-Preis des BvD sieht Richter als gute Ergänzung zum Journalistenpreis. Damit erhielten sowohl Text-Journalisten, als auch Kreative für Bewegtbild einen Anreiz, sich mit Einzelaspekten des Datenschutzes auseinanderzusetzen. Zugleich trügen sie damit Datenschutz in die Öffentlichkeit:

»Der DAME ist ein wichtiger Beitrag, das Bewusstsein der Zielgruppen zu stärken und zur Aufklärung über komplexe Datenschutz-Inhalte beizutragen«.

Klaus Müller, Vorstand Verbraucherzentrale Bundesverband



Klaus Müller ist seit Mai 2014 Deutschlands oberster Verbraucherschützer. Davor war der Grünen-Politiker Chef der Verbraucherzentrale Nordrhein-Westfalen. Bundesweit bekannt wurde er als Umweltminister von Schleswig-Holstein von 2000 bis 2005.

Aus seiner täglichen Arbeit beim Verbraucherzentrale Bundesverband weiß Müller, dass es eine große Herausforderung ist, wichtige, aber komplexe Themen wie den Datenschutz so zu vermitteln, dass Verbraucherinnen und Verbraucher aufhorchen.

»Datenschutz berührt unser aller Alltag. Doch nicht immer ist uns bewusst, wenn die Privatsphäre bedroht ist«, sagt Müller.

Oft sorgten abstrakte, schwer verständliche Datenschutzklauseln für Fragezeichen bei den Verbrauchern.

Dabei ist das Thema den Menschen nach Einschätzung Müllers grundsätzlich wichtig. »Fragen Sie Passanten auf der Straße doch einmal, ob Sie auf ihren Smartphones stöbern dürfen. Die meisten würden Sie für verrückt erklären.« Eingriffe in die Privatsphäre seien in der Regel nicht so offensichtlich, weil Daten im Hintergrund abgegriffen würden. »Hier kann eine bessere Aufklärung hilfreich sein«, sagt Müller.

Um die Aufmerksamkeit der Menschen zu wecken, hält er es für wichtig, neue Zugänge zu dem »sperrigen Thema Datenschutz« zu finden. Er hoffe, dass die Wettbewerbsbeiträge anschaulich machen, welchen Stellenwert Datenschutz in unserer digitalisierten Welt hat.

»Datenschutz ist kein Konzept von gestern. Und der Medienpreis ist ein Signal an die Datenkraken unter den Anbietern: Sie können sich nicht alles leisten, es schaut ihnen jemand auf die Finger.«

Müller räumte ein: »An vielen Stellen haben wir heute leider kaum mehr eine Wahl, ob wir unsere Daten zur Verfügung stellen oder nicht.« Aufklärung allein reiche nicht. »Wir brauchen bessere, verbraucherfreundliche Spielregeln«, forderte er. Zudem bedeute es nicht, dass es keine Entscheidungsfreiheit gebe. »Ich rate den Menschen, sich möglichst bewusst für oder gegen Güter und Dienste zu entscheiden.

»Man muss nicht jeden Trend mitmachen und nicht jede App installieren. Nicht jedes Gewinnspiel oder jede Kundenkarte ist es wert, sich dafür zu entblößen.«

Indem die Anbieter mit den persönlichen Daten handeln, würden die Kunden zu einem Produkt, das »verscherbelt« wird. »Gute Dienste sollten deshalb ruhig etwas kosten dürfen und dafür bleiben persönliche Daten unter Verschluss«, schlug Müller vor. Er selbst wolle die Kontrolle über seine Daten behalten. »Ich will bestimmen, was Unternehmen oder Behörden über mich wissen.«

»Ich engagiere mich für Datenschutz, weil ich die Kontrolle über meine Daten behalten möchte. Ich will bestimmen, was Unternehmen oder Behörden über mich wissen.«



Birgit Kimmel, EU-Initiative *klicksafe*, c/o Landeszentrale für Medien und Kommunikation Rheinland-Pfalz

Birgit Kimmel ist Medienreferentin in der Landeszentrale für Medien und Kommunikation in Rheinland-Pfalz und Pädagogische Leiterin der EU-Initiative »klicksafe«, die Kinder, Jugendliche, Eltern und Lehrkräfte neben vielen anderen Themen, auch über Datenschutz im Internet aufklärt.

Datenschutz ist für sie eine der Grundpfeiler von Demokratie und demokratischem Miteinander. »Dahinter verbirgt sich die ganz grundlegende Frage, zu was für einer Gesellschaft wir uns entwickeln werden, wenn wir nicht genau hinschauen, welche Folgen die Veräußerung persönlicher Daten haben kann«, sagt sie. Deshalb hält sie die Aufklärung der Nutzer über Datenschutz-Optionen und -Rechte für essentiell.

Bei Aktionen der Initiative »klicksafe« erlebt Kimmel im direkten Kontakt mit Jugendlichen und Erwachsenen immer wieder eine Diskrepanz zwischen dem Wunsch nach Privatsphäre auf der einen Seite und der bereitwilligen Preisgabe von persönlichen Daten auf der anderen Seite, etwa auf Facebook oder WhatsApp.

Einen Grund dafür sieht sie in der Abstraktheit von Daten und Datenverarbeitung.

»Was mit unseren Daten im Hintergrund passiert, wenn wir zuhause am Rechner sitzen, das bekommen wir ja eigentlich gar nicht mit«, sagt Kimmel.

Ein erster Schritt hin zu mehr Datenschutz ist für Kimmel die europäische Datenschutz-Grundverordnung, die ab 25. Mai 2018 von Unternehmen und Behörden angewendet werden muss. Dabei sieht sie vor allem die Politik in der Pflicht.

Daneben müssten die Bürgerinnen und Bürger stärker für die Verarbeitung ihrer persönlichen Daten im Alltag sensibilisiert werden. »Dazu brauchen sie mehr Informationen, vor allem verständliche und eingängige«, sagt Kimmel.

»Die Bürger und Verbraucher brauchen mehr Informationen, vor allem verständliche und eingängige.«

Dazu wird der DAME (Datenschutz Medienpreis) ihrer Einschätzung nach einen wichtigen Beitrag leisten. Denn über Videos und Clips lassen sich sehr unterschiedliche Zielgruppen erreichen – emotional und mit Beispielen aus der jeweils eigenen Lebenswelt. Zudem sind die Videos eng mit Youtube verbunden. »Youtube ist nach wie vor die zentrale Plattform, um Erklärfilme zu verbreiten«, sagt Kimmel.

Themen für die Beiträge könnten ihr zufolge beispielsweise die Datenschutzeinstellungen bei Facebook, Twitter & Co. sein, damit die User sie richtig nutzen könnten. »Da gibt es einige Möglichkeiten, die Privatsphäre zu schützen, aber oft ist das den Nutzern nicht bekannt.« Auch die Meldefunktion bei Facebook oder Instagram und deren Reaktionen auf Beschwerden sieht Kimmel als ein Thema.

Thomas Spaeing, Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.



Thomas Spaeing ist seit 2008 Vorstandsvorsitzender des BvD. Die Idee für den Datenschutz Medienpreis (DAME) entstand aus der Erfahrung der BvD-Initiative »Datenschutz geht zur Schule«. Mit Videos und kleinen Clips zeigen die Dozenten Kindern und Jugendlichen, was passieren kann, wenn sie unbedacht Daten und Fotos von sich ins Netz stellen.

»Auf Youtube gibt es mittlerweile eine Reihe von richtig guten Filmen und Videos von Netzaktivisten oder Künstlern, die sich mit Datenschutz auseinandersetzen«, sagt Thomas Spaeing.

Vor allem junge Leute ließen sich über solche Kanäle mit dem Thema Datenschutz erreichen.

»Die Beiträge müssen natürlich in der Sprache der Jugendlichen erzählt werden, und ohne den berühmten erhobenen Zeigefinger.«

Wichtig sei, dass die Bewerber für den Preis die meist komplexen Themen aus dem Datenschutz herunterbrächen auf konkrete Beispiele aus der Lebenspraxis der jeweiligen Zielgruppe. »Clips für Kinder sind natürlich anders gemacht als Hintergrundfilme für Unternehmen oder die Politik,« sagt Spaeing. »Aber bei den Einreichungen zählt die Idee, nicht das Budget.«

Mit dem Preis verbindet Spaeing die Hoffnung, mehr Menschen über die Veränderungen und Herausforderungen beim Datenschutz zu interessieren, vor allem zum Start der Datenschutz-Grundverordnung am 25. Mai nächsten Jahres. »Die neuen Regelungen betreffen ja nicht nur Datenschutzexperten in Unternehmen und Behörden, sondern auch Personal- und Abteilungsleiter, Geschäftsführungen, Betriebsräte, Senioren, Hausfrauen, Lehrkräfte und natürlich auch junge Leute«, sagt Spaeing. »Die DS-GVO berührt uns alle. Deshalb sehe ich es als unsere Aufgabe an, die komplexen Inhalte auch jenen zu erklären, die damit nicht wie wir jeden Tag befasst sind.«

Den ersten DAME-Award wird der BvD auf dem Verbandstag am 26. April 2018 verleihen, knapp einen Monat vor dem Start der europaweit gültigen DS-GVO.

»Ich bin überzeugt, dass wir gerade für Verbraucher und die Bürger einen wichtigen Beitrag zum Verständnis von Datenschutz und seiner Bedeutung für Wirtschaft und Verbraucher leisten werden«, sagte Spaeing.

Er ist auf alle Fälle sehr gespannt auf die Einsendungen.

Die Interviews führte Christina Denz für die BvD-News.

Anzeige

Wichtiges Datenschutzwissen für Ihre Kollegen

Mitarbeiterinformation zum Datenschutz

Kommen Sie Ihrer Verpflichtung zum Datenschutz nach und schulen Sie Ihre Mitarbeiter mit der kompakten Infobroschüre.

Profitieren Sie von unseren BVD-Staffelpreisen:

→ Einzelpreis für BVD-Mitglieder	6,98 €/Stk.
→ 10-50 Stk. für BVD-Mitglieder	4,87 €/Stk.
→ 51-100 Stk. für BVD-Mitglieder	4,13 €/Stk.
→ 101-500 Stk. für BVD-Mitglieder	2,17 €/Stk.

BvD-Rabatt
30%

TKMmed!a



INDIVIDUALISIEREN

Sie Ihre Infobroschüre mit Ihrem eigenen Firmenlogo und den Kontaktdaten des Datenschutzbeauftragten!



Jetzt **HIER** persönliches Angebot anfordern:
mib@datenschutz-aktuell.de

WETTBEWERBSVORTEIL: TRANSPARENTE ANSPRACHE

Sebastian Himstedt

Stiftung Datenschutz gibt Handreichung für bessere Datenschutzkommunikation heraus

Die Sicherheit der eigenen Daten und der Schutz der Kundendaten gehört zum Geschäftsmodell digitaler Dienstleister. Für Julia Röbbke, Projektmanagerin für Software und Digitale Prozesse der COMDOK GmbH, einem IT-Dienstleister mit Sitz in St. Augustin und Berlin, der u. a. für öffentliche Einrichtungen und Organisationen wie Stiftungen und Verbände arbeitet, ist sie ein elementarer Bestandteil ihrer täglichen Arbeit. »Wir haben ein stark datenbasiertes Geschäft. Somit sind wir auf klar strukturierte und praktische Lösungen angewiesen, um unsere Kundendaten zu schützen.« Doch längst haben nicht alle kleinen und mittleren Unternehmen die Wichtigkeit des Datenschutzes für ihr Geschäftsmodell erkannt.

Die Wahrnehmung von datenschutzrechtlichen Problemstellungen entwickelt sich jedoch schrittweise weg von einem Instrument zur Verhinderung von Projekten hin zu einer unmittelbaren Voraussetzung guter Unternehmensführung und einem Fundament für geschäftlichen Erfolg. Dies geschieht zwar nur in kleinen Schritten, aber doch merklich. Datenskandale und die NSA-Enthüllungen haben Kunden sensibler gemacht. Das Vertrauen im B2B-Verkehr ist dann am größten, wenn Geschäftspartner keine Sicherheitslücken darstellen. Datenschutz und Datensicherheit gehen somit Hand in Hand. »Aus unserer Sicht ist Datenschutz so etwas wie das neue Bio-Siegel. In ein paar Jahren wird ein souveräner Datenumgang zu einem wichtigen Prozess eines jeden Unternehmens gehören,« skizziert Frederick Richter, Vorstand der Stiftung Datenschutz, den Wandel. Gerade datenorientierte Unternehmen mit starkem Onlinegeschäft können es sich nicht mehr leisten, das Thema zu vernachlässigen.

Demzufolge wird auch die Kommunikation zum Datenschutz und seiner Umsetzung immer wichtiger. Vielen Anbietern machen allein schon die Formulierungen der Datenschutzbestimmungen auf ihren Websites Sorgen. Speziell für kleinere und mittlere Unternehmen hat die Stiftung Datenschutz deshalb ein Angebot zusammengestellt, das die Informationslücke in der richtigen Ansprache von Zielgruppen in Fragen des Datenschutzes schließt. Die Handreichung »Kommunikation von Datenschutz – Recht und (gute) Praxis« der Stiftung Datenschutz schildert die einzuhaltenden rechtlichen Vorgaben und hilft, komplexe Sachverhalte für Kunden und Geschäftspartner einfach und klar zu benennen. Erweiternd zu dieser ersten Hilfestellung für Unternehmen werden zukünftig in zusätzlichen Beispieltexten und übersichtli-



chen Grafiken Möglichkeiten einer vorteilhaften und überzeugenden Kommunikation aufgezeigt werden. Dazu sollen in späteren Versionen auch Best-Practice-Beispiele vorgestellt und Diskussionsangebote geschaffen werden. Vorstellbar wäre auch ein Online-Lexikon, in dem einzelne Nutzer Inputs geben und verändern können.

Unterstützt wurde die Stiftung Datenschutz dabei von zwei starken Partnern: Dirk Pohl und Prof. Dr. Kai von Lewinski von der Universität Passau steuerten einen wesentlichen Teil der Inhalte bei, während die DATEV Stiftung Zukunft die Arbeit der beiden Wissenschaftler unterstützte.

Das Ziel der Handreichung ist schon im Titel beschrieben: Es soll das manchmal sehr theoretische Recht in eine bessere Praxis überführt werden. Dafür wurden anwendungsbezogene Beispiele gewählt, die sich besonders an kleine und mittelständische Unternehmen richten.

Besonderer Wert bei der Darstellung wurde auf praktische Fragen gelegt. Ein zentrales Problem dabei ist beispielweise die Einwilligung in die Datennutzung. Neben der Verarbeitung von Daten auf Grundlage einer gesetzlichen Erlaubnis besteht die Möglichkeit, darüber hinaus Daten mit Einwilligung des Betroffenen zu verarbeiten. Viele Unternehmen stellen sich hier die Frage, wer wann wem das Recht zur Nutzung erteilt und für wie lange dies geschieht. Oft kommt es an diesem Punkt entweder zu überlangen, unverständlichen Erklärungen, die vom Kunden einfach weggeklickt werden, oder schlichtweg zu nicht rechtssicheren Lösungen.

Die Kommunikation über die Erfüllung der rechtlichen Pflichten hinaus ist aber äußerst lohnenswert. So kann sich der Bearbeiter nämlich die Erlaubnis für die Verarbeitung weiterer Daten und in zusätzlichen Kontexten erschließen, die er sonst nicht verarbeiten dürfte.

»Für unsere Kunden ist es enorm wichtig zu wissen, dass ihre Daten bei uns sicher und auf inhouse betriebenen Servern gespeichert werden«, berichtet auch Julia Röbbke von der COMDOK GmbH. Mit eigenen Servern ist das Unternehmen für ein Angebot rund um CRM-System, Webhosting und Systemadministration gut aufgestellt. Diese Fragen seien vor Jahren in dieser

Intensität noch nicht relevant gewesen. Da der Aufbau einer umfassenden Datenschutzstruktur für kleinere und mittlere Unternehmen eine Hürde darstellt, ist man auf praktische Hilfestellungen angewiesen. Das bestätigt auch Julia Röbbke: »Wir werden bei der COMDOK das Thema noch stärker in den Fokus rücken, weil Datensicherheit und Datenschutz zum Markenkern gehören und für alle Produkte und Services relevant sind.« Die Handreichung der Stiftung Datenschutz kann dazu beitragen, die Kommunikation und das Verständnis der Kunden in diesem Bereich zu verbessern. Sie steigert somit nicht nur das Ansehen des Datenschutzes, sondern hilft ebenfalls dabei, ein gleichberechtigtes Miteinander in der Wirtschaft zu schaffen.

Die Broschüre ist abrufbar auf www.stiftung-datenschutz.org/ds-kommunikation



Über den Autor

Sebastian Himstedt

35 Jahre alt, nach Stationen bei ARD, WDR und der Neuen Osnabrücker Zeitung sowie im Deutschen Bundestag arbeitet er als freier Journalist in Berlin.



DATENSCHUTZ-COMPLIANCE NACH DER DS-GVO

Kranig, Sachs, Gierschmann



KRANIG, SACHS, GIERSCHMANN
Datenschutz-Compliance nach der DS-GVO

Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden

Bundesanzeiger Verlag

1. Auflage 2017, 230 Seiten
ISBN-13: 978-3846207604
44,00 Euro

Das Werk bietet Hilfestellungen und Vorgabemuster für die Datenschutzorganisation und richtet sich explizit an Verantwortliche der Datenverarbeitung. Das Autorenteam setzt

sich aus dem Präsidenten des Bayerischen Landesamtes für Datenschutzaufsicht (BayLDA), dem Leiter des Referats Technischer Datenschutz und IT-Sicherheit des BayLDA und einem auf Datenschutzmanagement spezialisiertem Unternehmensberater zusammen. Diese Mischung aus Jurist, Diplom-Informatiker und Diplom-Wirtschaftsingenieur betrachtet die DS-GVO aus Compliance-Sicht.

Explizite Zielgruppe des Werkes sind die Verantwortlichen, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheiden. Auftragsverarbeiter sind nicht konkret adressiert, werden aber auch nicht abgehalten, sich mit diesen Sichtweisen zu befassen.

Das Werk umfasst drei Teile: Einführung in die DS-GVO, Sicherstellung der Datenschutz-Compliance und Überwachung der Datenschutz-Compliance. Im ersten Teil wird deutlich hervorgehoben, dass die Unternehmensleitung die Verantwortung für eine regelkonforme Umsetzung der rechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten trägt. Ein Umstand, der erst jetzt durch die Datenschutz-Grundverordnung und deren Sanktionsmöglichkeiten allen Managementebenen eines Unternehmens bewusst zu werden scheint. Die dabei wesentlichen Datenschutzprozesse der datenschutzkonformen Datenverarbeitung, der Sicherstellung der Betroffenenrechte und die Handhabung von Datenschutzverletzungen werden dabei als Teil der Ablauforganisation dargestellt. Die Aufbau-

organisation mit den Datenschutzstrukturen über Datenschutzziele, Datenschutz-Governance-Struktur sowie der Datenschutzleitlinie bildet den weiteren Schwerpunkt des übersichtsartigen ersten Teils.

Im zweiten Teil finden sich dann detaillierte Ausführungen zu den Datenschutzprozessen der Ablauforganisation wieder. Unterstützt von vielen grafischen Abbildungen werden anschaulich die Organisationabläufe der einzelnen rechtlichen Anforderungen erläutert. Neben dem Datenschutz-Risikomanagement umfasst dies die Datenschutzdokumentation, die Sensibilisierung zum Datenschutz, die Thematik des Datenschutzaudits / bzw. der Datenschutzzertifizierung sowie das Datenschutz-Managementsystem. Ein dabei immer wieder eingeforderter Prozessschritt ist der PDCA-Zyklus (plan-do-check-act), der in vielen Organisationsstrukturen bereits z. B. bei der Informationssicherheit implementiert ist.

Die Ausführungen zum Risikomanagement beinhalten eine detaillierte Darstellung der Anforderungen an einen risikobasierten Ansatz und an einen Risikomanagementprozess. Die Matrix zur Risikobewertung folgt den Festlegungen in der ISO 29134 und wird durch anschauliche grafische Abbildungen gut nachvollziehbar vermittelt. Hinsichtlich der Umsetzung einer Datenschutz-Folgenabschätzung werden die Schritte zur Risikoidentifikation, der Risikoanalyse und der Risikoevaluation erläutert, bevor dann die Ausführungen zu den Risikobehandlungsoptionen folgen. Auch den in der DS-GVO gestiegenen Dokumentations- und Nachweispflichten (vgl. Art. 5 Abs.2) wird durch tabellarische Aufliste der Dokumentationsanforderungen und grafischen Darstellungen Rechnung getragen.

Im abschließenden dritten Teil werden die Befugnisse der Aufsichtsbehörden dargelegt, bevor durch mehreren Prüffragen zu den einzelnen Maßnahmen eine Selbstprüfung ermöglicht wird.

Das Buch ist uneingeschränkt empfehlenswert, fasst es doch in überschaubarem Umfang die wichtigsten prozessualen Anforderungen an die Umsetzung der DS-GVO zusammen. Die vielen grafischen Darstellungen erleichtern die Komplexität der Zusammenhänge zu erfassen. Auch wenn sich das Buch explizit nur an den für die Datenverarbeitung Verantwortlichen richtet, hilft es auch dem Datenschutzbeauftragten, den Verantwortlichen effektiv zu beraten.

DS-GVO DATENSCHUTZ-GRUNDVERORDNUNG VO (EU)

Gola (Hrsg.)



GOLA (HRSG.)

DS-GVO Datenschutz-Grundverordnung VO (EU) 2016/679, Kommentar

C.H. Beck-Verlag

1. Auflage 2016, 835 Seiten
ISBN-13: 978-3406695438
79,00 Euro

Bei den Regelungen des BDSG zählte der Gola/Schomerus zum Standardkommentar des deutschen Datenschutzrechts. Über 12 Auflagen hinweg war »der Gola« ein hilfreicher, kompakter Begleiter zu den relevanten Fragestellungen des BDSG.

An diese Tradition möchte diese Kommentierung anknüpfen: Umfang und Aufmachung orientieren sich am Vorgänger, das Autorenteam hat sich teilweise geändert: Vertreter von Wissenschaft, Praktiker, Vertreter der Wirtschaft und der Aufsichtsbehörden stellen das Autorenteam (vielleicht erfahre ich eines Tages, wie sich Praktiker definieren, die weder Vertreter der Wirtschaft noch der Aufsichtsbehörden sind). Aus der besonderen Nähe einiger Autoren zur Gesellschaft für Datenschutz und Datensicherheit (nicht mehr »Datensicherung« wie auf dem Schutzumschlag vermerkt) steigt die Erwartung, dass insbesondere praxisnahe Erläuterungen zu finden sind. Hatte der bisherige Kommentar zum BDSG mit seinen insg. 63 Paragraphen noch einen Umfang von 677 Seiten, werden nun für 99 Artikel der Grundverordnung mit den 177 Erwägungsgründen insgesamt 835 Seiten genutzt.

Nach Wiedergabe der Artikel der DS-GVO samt Erwägungsgründen folgt über 20 Seiten eine Einleitung, die einen guten Überblick über Entstehungsgeschichte, Einzelregelungen und offen gebliebenen Fragestellungen zur DS-GVO bietet. Besonders ausführlich und trotz des frühen Redaktionsschlusses sehr umfassend werden die Rechtmäßigkeitsgrundlagen des Art. 6 dargestellt. Auch die neuen rechtlichen Vorgaben zur Einwilligung eines Kindes in Bezug auf die Dienste der Informationsgesellschaft (Art. 8) werden nachvollziehbar diskutiert, kritische Bewertungen angesprochen und – soweit zu diesem frühen Stadium möglich – Lösungsmöglichkeiten aufgezeigt.

Tabellarische Übersichten wie bei Art. 12 oder Art. 15 erleichtern den Überblick für Zusammenhänge einzelner Normen. So kann beispielsweise über die bei der Kommentierung in Art. 15 dargestellte tabellarische Form der Inhalte der Informations- und Auskunftspflichten die Entscheidung unterstützt werden, ein Verzeichnis der Verarbeitungstätigkeiten trotz Art. 30 Abs.5 auch als KMU zu führen. Über das Verzeichnis der Verarbeitungstätigkeiten können dann die Informationen abgeglichen werden, welche in der Tabelle als Informations- und Auskunftspflichten übersichtlich aufgeführt werden.

Bei den Ausführungen zur Auftragsverarbeitung in Art. 28 hätten u. a. die Fragestellungen, die sich aus dem Wegfall des §11 Abs.5 BDSG ergeben, ausführlicher diskutiert werden können, auch unter Verweis auf die Darstellung der Thematik unter Art. 4 Nr. 8.

Die Darstellung des »risikobasierten Ansatzes« erfolgt in Art. 24, um dann in Art. 32 darauf zu verweisen und um auf dieser Basis die erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutzniveau der Rechte und Freiheiten der natürlichen Person danach auszurichten.

Für den frühen Veröffentlichungszeitpunkt überraschend gut sind die Ausführungen zur Datenschutz-Folgenabschätzung geworden, die einen strukturierten Überblick zur Historie, Herangehensweise und Durchführung geben.

Dem frühen Redaktionsschluss des Werkes ist es geschuldet, dass so hilfreiche Übersichten wie die zu Art. 88 und zu den Regelungen zum Beschäftigtendatenschutz durch die künftige Neufassung des BDSG (dort §26 BDSG n.F.) hinsichtlich der Aussagekraft neu bewertet werden müssen. Bei einer Gesamtbewertung darf nicht verkannt werden, dass bei dem frühen Redaktionsschluss weder die ersten Leitlinien der Art.-29-Datenschutzgruppe noch andere Kommentare zur Verfügung standen, die bei einer Darstellung der rechtlichen Interpretation insbesondere zu den neuen Formulierungen der DS-GVO herangezogen werden konnten. Der »neue Gola« kann die Tradition als »Klassiker« fortsetzen, wenn es gelingt, insbesondere die neueren Regelungsbereiche in der Kommentierung in den folgenden Auflagen durch die bis dahin gewonnenen Erkenntnisse zu ergänzen. Für den Einstieg in die Welt der DS-GVO ist der »Gola« ein nützlicher und empfehlenswerter Begleiter, der Fachbücher zu konkreten Themen und weitere Kommentare mit seinem handlichen Format sinnvoll ergänzt.

DATENSCHUTZ-GRUNDVERORDNUNG

Ehmann / Selmayr (Hrsg.)



EHMANN / SELMAYR (HRSG)

Datenschutz-Grundverordnung

C.H. Beck Verlag

1. Auflage 2017, 1.243 Seiten
ISBN-13: 978-3406702150
139,00 Euro

Ein weiterer Kommentar zur Datenschutz-Grundverordnung aus dem C.H. Beck-Verlag liegt vor, der die Diskussion um die Interpretation der europaweiten Auslegung bereichert.

Als Herausgeber agieren der Regierungsvizepräsident der Regierung von Mittelfranken, Dr. Eugen Ehmann, der u. a. schon als Kommentator der RL 95/46 in Erscheinung trat und Prof. Dr. Martin Selmayr, Kabinettschef des Präsidenten der Europäischen Kommission und Direktor des Centrum für Europarecht an der Universität Passau. Die Herausgeber nutzten ihr europäisch- / bayrisch-geprägtes Netzwerk, um sowohl Akteure aus dem Gesetzgebungsverfahren, Praktiker aus Aufsichtsbehörden und Wirtschaft sowie Vertreter der Wissenschaft als Kommentatoren zu gewinnen.

Das Ergebnis ist ein vielseitiges Werk, dessen Umfang und Tiefe den Anforderungen gerecht wird.

Nach der Wiedergabe des vollständigen Verordnungstextes folgt eine über 70-seitige Einführung, welche die Entstehung des europäischen Datenschutzes und insbesondere der DS-GVO umfassend darstellt. Besonders hervorhebenswert sind hierbei die Ausführungen zur Auslegung der DS-GVO als Unionsrecht, da sie auch dem in europarechtlichen Fragen ungeübten Datenschützer wichtige Leitlinien mitgeben.

Die Bearbeitungen der einzelnen Artikel folgen einer klaren Struktur, die eine systematische Befassung mit den Regelungen erleichtern.

Bis auf die Erläuterung zu den personenbezogenen Daten wirken die Darstellungen der Begriffsbestimmungen zusammengefasst dargestellt. Die Ausführungen zu den Grundsätzen und Rechtmäßigkeitsvoraussetzungen sind umfassend und detailliert umgesetzt. Die Betroffenenrechte werden ausführlich erörtert. Es fiel auf, dass sich offensichtlich die Herausgeber bei den Formulierungen der Kommentatoren zurückhielten, da der Begriff der »Öffnungsklausel« zugunsten der Mitgliedstaaten immer wieder verwendet wird und zumindest einer der Herausgeber bekanntermaßen lieber den Begriff der »Spezifizierungsklausel« bzw. »Spezifizierungsbefugnis« verwendet.

Bei der Kommentierung zu den Vorgaben zur Auftragsverarbeitung fallen die praxisnahen Hinweise zur Gestaltung positiv ins Auge. Auch wenn die Erörterungen der Begrifflichkeit in Art. 32 zu den Risiken für die Rechte und Freiheiten natürlicher Personen ausführlicher hätten ausfallen können, bildet die Kommentierung zu Kapitel IV alle wesentlichen Fragestellungen, die sich derzeit durch die DS-GVO ergeben, ab. Insbesondere bei der Datenschutz-Folgenabschätzung wird der zum Zeitpunkt des Redaktionsschlusses bekannte Stand gut dargestellt. Auch die Befassungen mit den Themenbereichen der Zertifizierungen und genehmigten Verhaltensregeln können gut in der Praxis bei komplexen Fragestellungen herangezogen werden. Umfassend und vertieft dargestellt werden die Regelungen in Kapitel VI zu den Aufsichtsbehörden. Insbesondere vor dem Hintergrund der Diskussionen um den § 29 Abs.3 BDSG n.F. und der dortigen Umsetzung der Regelungsmöglichkeit zu den Befugnissen der Aufsichtsbehörden gegenüber Berufsheimnisträgern liest sich die Kommentierung zu Art. 90 erhellend.

Insgesamt ein handlicher und umfassender Kommentar, der in der Praxis wertvolle Hilfe leisten kann, auch durch den Blickwinkel der »europäischen Brille« ohne die bisherige deutsche Rechtsentwicklung aus dem Auge zu verlieren.

DATENÜBERMITTLUNG IM KONZERN

Matthias Lachenmann



MATTHIAS LACHENMANN
»Datenübermittlung im Konzern«

Oldenburger Verlag für Wirtschaft, Informatik und Recht

1. Auflage 2016, 398 Seiten
 ISBN-13: 978-3955990336
 49,80 Euro

Das Werk umfasst die 2016 an der Carl von Ossietzky Universität Oldenburg verfasste Dissertation des Autors. Zwar bezieht sie sich vorwiegend auf die Rechtslage unter dem BDSG,

hat aber schon den Blick auf die Regelungen unter der DS-GVO gerichtet.

In vier Kapiteln werden die »normative Grundlagen der Datenverarbeitung im Konzern« (Kapitel 1), die »Durchführung der Datenübermittlung im Konzern« (Kapitel 2), die »künftige Aufstellung der Datenübermittlung im Konzern« (Kapitel 3) sowie die »Ergebnisse« (Kapitel 4) dargestellt.

Die Behandlung der Datenübermittlung innerhalb von Konzernen war und bleibt immer ein aktuelles Thema, das mit vielerlei Fragestellungen behaftet ist. So werden im ersten Kapitel die Grundlagen dargestellt, die sowohl den Personenbezug, wie auch die Zulässigkeitsvoraussetzungen umfassen. Die Probleme, die sich aus dem fehlenden »Konzernprivileg« ergeben, werden anschaulich dargestellt und auch die historische Entwicklung der Thematik sowie das Verhältnis zu gesellschaftsrechtlichen Aspekten beleuchtet.

Die verschiedenen Varianten einer Datenweitergabe im Konzern werden im zweiten Kapitel zunächst an der Auftragsverarbeitung herausgearbeitet, wobei hier ausführlich auch auf die unterschiedlichen Auslegungstheorien zur Auftragsverarbeitung eingegangen wird. Einen schönen Schwerpunkt nimmt die Darstellung der Datenübermittlung an Konzernunternehmen innerhalb Deutschlands ein. Hierbei werden die in Frage kommenden Zulässigkeitsvoraussetzungen wie Einwilligung und die Zulässigkeitsvoraussetzungen nach den §§ 28, 29 BDSG bis hin zu § 32 BDSG erörtert. Auch die Möglichkeiten über Verhaltensregeln nach § 38a BDSG werden angesprochen.

Bei der Thematik der Datenübermittlung an Konzernunternehmen außerhalb Deutschlands werden die Kritikpunkte an der Europarechtswidrigkeit des Ausschlusses der Auftragsdatenverarbeitung in Drittstaaten ausgeführt und die denkbaren Möglichkeiten zum Datentransfer in »unsichere Drittstaaten« aufgeführt.

Im dritten Kapitel wird die Thematik auf Basis der DS-GVO behandelt und das Werk entwickelt sich auch dadurch zum »zukunftsfesten« Begleiter für die datenschutzrechtlichen Fragestellungen zur Datenübermittlung im Konzern auch unter der DS-GVO. So finden sich beispielsweise in den Ausführungen zur künftigen Aufstellung der Datenübermittlung nachvollziehbare Ausführungen zur Geltung des Widerspruchrechts nach Art. 21 DS-GVO, eine plausible Begründung für die Beibehaltung der Privilegierungswirkung bei der Auftragsverarbeitung und Ausführungen zur Gestaltung nach Art. 26 DS-GVO (Gemeinsam für die Verarbeitung Verantwortliche).

Im abschließenden vierten Kapitel wird anhand von 11 Thesen das Ergebnis der Arbeit dokumentiert, welche dann in insgesamt 57 Punkte zusammengefasst werden.

Auch wenn man dem Werk nicht in allen Aussagen zustimmen muss (ich habe beispielsweise etwas meine Schwierigkeiten mit der 3. These und den dortigen Ausführungen zur Betriebsvereinbarung als Erlaubnistatbestand), bietet es eine umfassende Darstellung aller relevanten Fragestellungen zum Datentransfer im Konzern und behandelt auch die Thematiken der DS-GVO. Für eine wissenschaftliche Arbeit bietet sie eine überraschende Praxisnähe und auch durch den leicht verständlichen Sprachstil empfiehlt es sich für jeden, der sich mit Datenübermittlung im Konzern zu befassen hat.

Rezensionen von

Rudi Kramer

Stellv. Vorstandsvorsitzender des BvD



BvD^{e.V.}
 DATENSCHUTZ GESTALTEN

RECHTSHANDBUCH BETRIEBLICHER DATENSCHUTZ

(Forgó/Helfrich/Schneider)



FORGÓ/HELFRICH/SCHNEIDER
Betrieblicher Datenschutz

C.H. Beck Verlag

2. Auflage 2017, Buch, LX,
1331 S. Hardcover (In Leinen)
ISBN 978-3-406-69541-4
Format (B x L): 16,0 x 24,0 cm

Das hier rezensierte Werk ist kein Handkommentar zum Datenschutz, sondern vielmehr ein Handbuch zum Datenschutzrecht, welches sehr umfassend und anschaulich darstellt, wie insbesondere das neue Datenschutzrecht in den

typischen Verarbeitungssituationen anzuwenden ist. Erfreulicherweise beschränken sich die Autoren nicht auf typische Verarbeitungen, sondern beleuchten auch viele Spezialfälle sehr konkret und diskutieren dabei auch die Implikationen aus anderen Rechtsgebieten. Zahlreiche Beispiele erleichtern die Handhabung der komplexen Themen und bieten dem Leser einen schnellen Einstieg in das jeweilige Thema und liefert damit insbesondere auch internen und externen Datenschutzbeauftragten eine wertvolle Hilfestellung dabei, sich die weniger typischen Verarbeitungstätigkeiten für ihre datenschutzrechtliche Beratung zu erschließen.

Soweit das jeweilige Thema es erfordert, werfen die Autoren dabei auch einen Blick über die Landes- und EU-Grenzen, um ein Verständnis der Datenschutzregelungen in anderen insbesondere Drittstaaten zu ermöglichen.

Das Autorenteam besteht aus anerkannten Datenschutzexperten, die sich dankenswerter Weise auch die Zeit genommen haben, den einen oder anderen Fachbegriff noch einmal grundlegend zu erläutern. So hat der Leser den zusätzlichen Vorteil, die heute oft sehr pauschal verwendeten Begrifflichkeiten bspw. für heute typische Technologien konkret nachzuschlagen, um Missverständnisse zu vermeiden.

Zu beachten ist, dass das Werk die datenschutzrechtliche Situation auf Basis der DS-GVO und des BDSG in heute geltender Fassung untersucht. Das BDSG-neu konnte aufgrund des Erscheinungsdatums nicht berücksichtigt werden. Trotzdem gibt das Rechtshandbuch wichtige Hinweise zur Anwendung der DS-GVO für die Übergangszeit und die Umstellungsprojekte. Insofern handelt es sich um ein hilfreiches Werk, welches in keinem Umstellungsprojekt fehlen sollte.

Rezension von

Thomas Spaeing

Vorstandsvorsitzender BvD



BvD^{e.V.}

DATENSCHUTZ GESTALTEN

WEITERHIN DS-GVO IM BLICK – MITGLIEDERBEFRAGUNG 2017

Dr. Kai-Uwe Loser

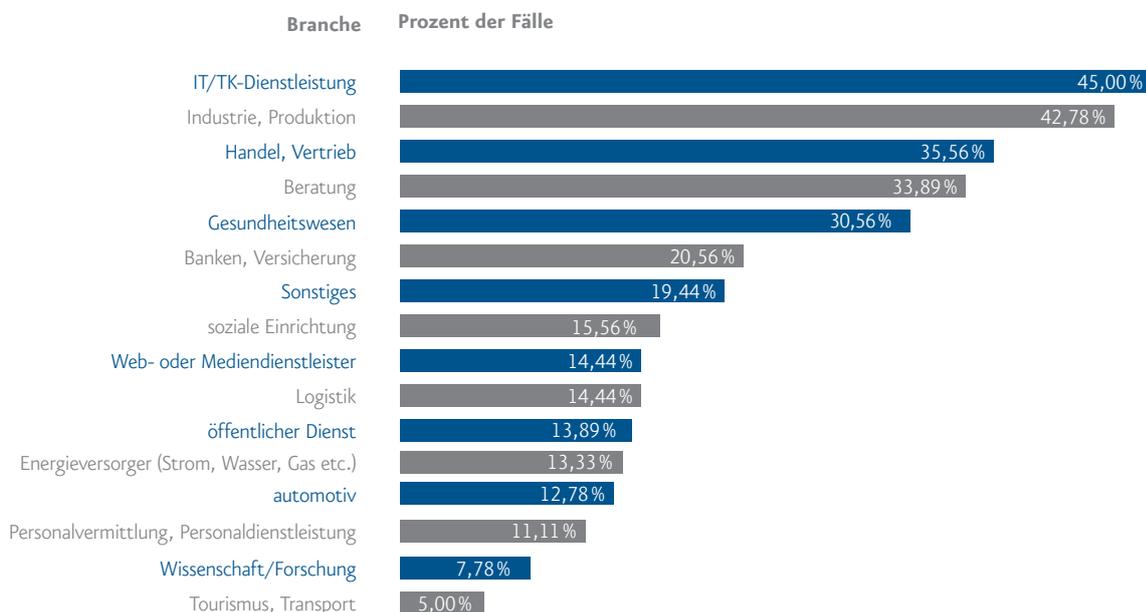
Ende 2016/Januar 2017 wurde entsprechend eines zweijährigen Turnus nun zum dritten Mal eine Mitgliederbefragung durchgeführt. Ziel einer Aktualisierung der Daten zu den Mitgliedern, die auch bei einer Außenbeurteilung des Verbands wesentlich sind: An vielen Stellen müssen wir beantworten, wen der BvD denn eigentlich vertritt. Nachdem der Verband nun die 900-Mitglieder-Grenze überschritten hat, ist das realistische Ziel nun die Eintausender-Marke zu erklimmen. Ca. 180 Mitglieder haben an der Befragung teilgenommen. Das ist weiterhin eine erfreulich hohe Zahl. Von den beantwortenden sind 59 % nur als Externe tätig, 28 % nur interne, 8 % geben beides an. Insgesamt 48 % sind selbständig.

Vertretene Branchen

Die Frage nach den vertretenen Branchen zeigt die Breite des Verbands. Hier ist erkennbar, dass aus allen Branchen, Sparten und Bereichen Vertreter im Verband organisiert sind. Einerseits ist das wesentlich für die Legitimation unserer politischen Beteiligung. Rückmeldungen können sich aus vielen Branchen speisen. Andererseits ist das wesentlich für die eigene Organisation: Für bestimmte Branchen werden Arbeitskreise organisiert. Hinweise darauf, für welche Branchen weitere sinnvoll wären, sind in der Betrachtung der Ergebnisse erschließbar. Es gibt dabei eine

Gruppe in der 30 % und mehr der Mitglieder tätig sind. Das sind die Branchen IT und IKT, Industrie/Produktion, Handel /Vertrieb, Beratung und Gesundheitswesen. Je zwischen 10 und 25 % der Mitglieder sind in den Branchen Banken/Versicherungen, Soziale Einrichtungen, Logistik, Web und Medien, öffentlicher Dienst, Energieversorger und der Automobilbereich. Sinnvoll können sicherlich noch Arbeitskreise im Bereich IT-Dienstleister oder auch für den öffentlichen Dienst sein. Hier sind auch die Mitglieder aufgerufen aktiv zu werden.

Mitgliederbefragung – Vertretene Branchen

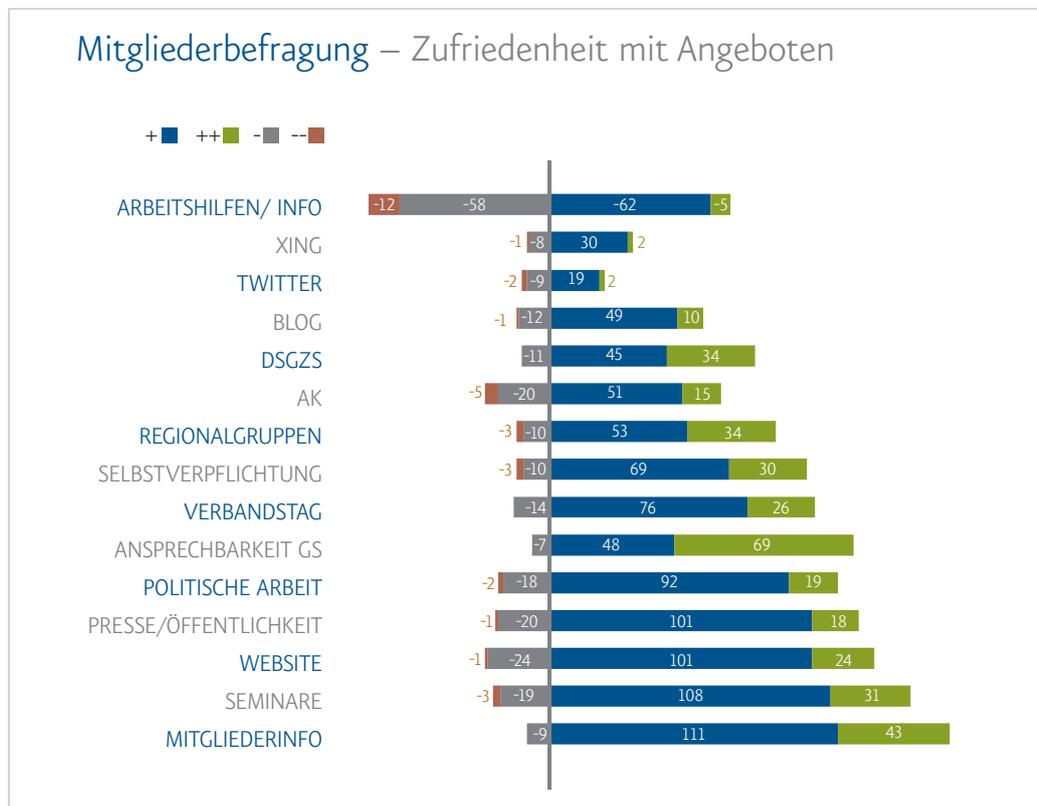


Bewertung der Verbandsarbeit

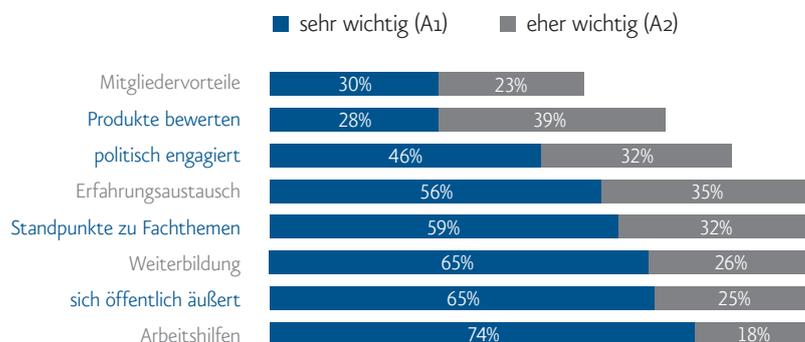
Ähnliches Feedback hat sich der Verband auch für evaluative Fragen bezgl. der verschiedenen Leistungen bzw. den Tätigkeitsbereichen des Verbands erhofft.

Hier zeigt sich die Arbeit zunächst als positiv bewertete Informationsquelle. Die Mitgliederinfo wird sehr positiv beurteilt, die Seminare ebenso wie Presse und politische Arbeit. Die Ansprechbarkeit der Geschäftsstelle wird äußerst positiv beurteilt. Noch nicht angekommen sind verschiedene weitere digitale Kanäle, wie XING,

Twitter oder der Blog. Diese erhalten zunächst einmal wenige Rückmeldungen, was bedeutet, dass diese von Mitgliedern nicht angenommen werden. Arbeitshilfen und Infomaterialien erhalten sehr viele negative Beurteilungen. (Neu-) Mitglieder erhoffen sich hier mehr vom Verband. Das zeigt sich auch in der Frage zur subjektiven Wichtigkeit der einzelnen Tätigkeitsbereiche. Bisher ist es dem Verband, der sich aus ehrenamtlicher Tätigkeit speist, nicht gelungen hier größere und zufriedenstellende Umfänge zu erreichen. Daher sei auch an dieser Stelle dazu aufgerufen hier mitzuarbeiten.



Mitgliederbefragung – Wichtigkeit der Angebote des BvD

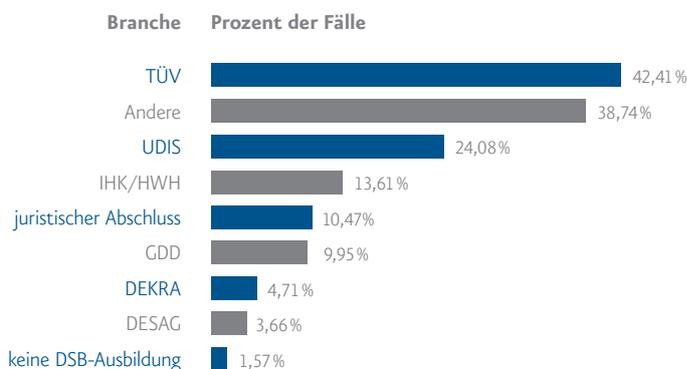


Ausbildung von Datenschutzbeauftragten

Die Ausbildungen sind vielfältig. Der TÜV dominiert die Ausbildungen zum DSB mit über 40%. Das hat wohl am ehesten mit der Bekanntheit des Namens in der öffentlichen Wahrnehmung zu tun. Ein Viertel der (antwortenden) Mitglieder haben eine Ausbildung bei der UDIS absolviert. Weitere liegen dann bei ca. 10%, etwa IHK, GDD oder die juristischen Abschlüsse.

Es bleibt ein unklarer Bereich von 38 %, die »Andere« angeben. Mit Blick auf Aussagen im Berufsbild der Datenschutzbeauftragten, das der Verband regelmäßig aktualisiert, sind das nützliche Informationen. Zum einen lässt sich daran ablesen, woher wir als Verband kommen, andererseits stellt sich die Frage, welche Veränderungen wesentlich sind, auch um den Verband als »Qualitätsmerkmal« zu etablieren.

Mitgliederbefragung – Datenschutzbeauftragten Ausbildung

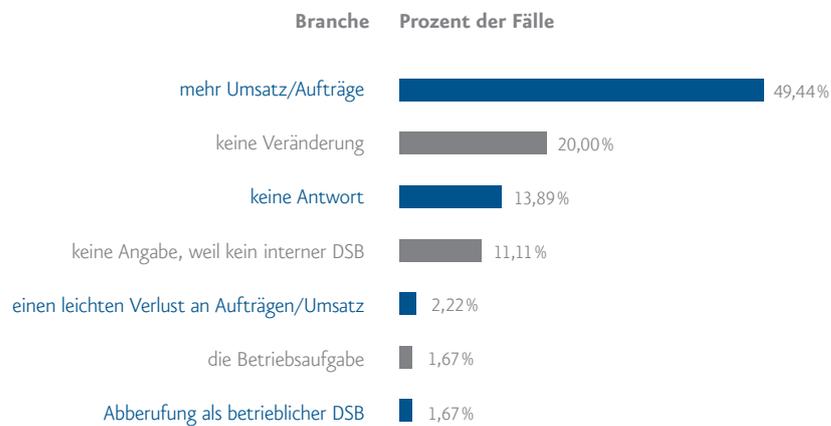


Die Mitglieder und die DS-GVO

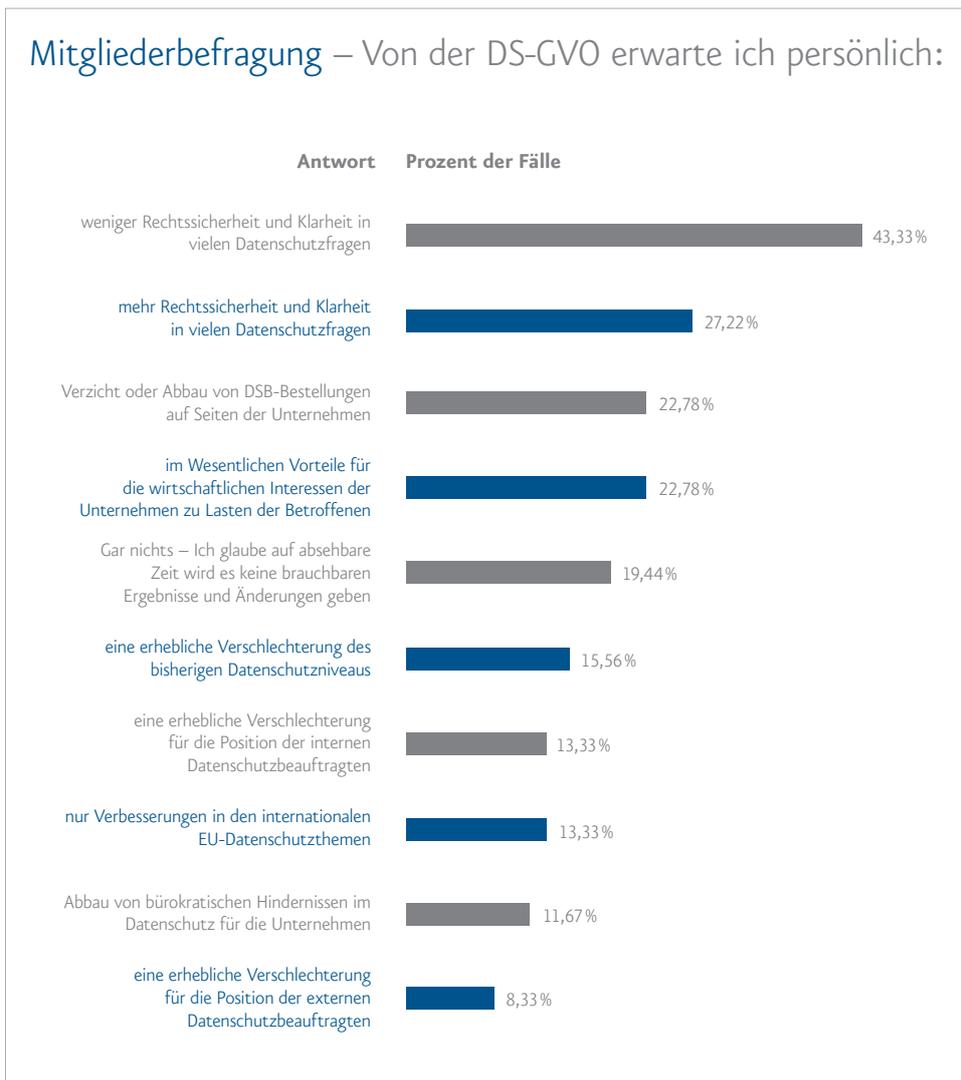
Nicht überraschend bleibt das Thema DS-GVO sehr präsent bei den Mitgliedern. Es wurde offen nach Qualifizierungsbedarfen gefragt, in denen sich Mitglieder weiterbilden lassen wollen. Von 124 Nennungen sind 37 EU-Datenschutz-relevant. Einige betreffen spezielle Regelungen wie bspw. Folgenabschätzung oder Datenschutzmanagement. Die Selbsteinschätzung in diesem Wissensbereich ist im Vergleich zur Befragung in der unsicheren Situation von 2014 bereits erheblich verbessert, aber im Vergleich zu anderen Wissensbereichen noch weiter verbesserungsfähig. Zu diesem Thema wurde etwas detaillierter nach einer Selbsteinschätzung gefragt. Hier fallen die Bereiche Risikoabschätzung/Folgeabschätzung, Datenschutz durch Technikgestaltung auf. In diesen Bereichen er-

kennen viele Mitglieder für sich noch Nachholbedarfe. Vom Allgemeinen geht das Interesse dabei also nun deutlich in die spezielleren Fragestellungen. Abschließend ist festzustellen, dass die Mitglieder wesentlich positiver in ihre eigene Zukunft schauen. Während in der unsicheren Situation 2014 einige um ihre berufliche Existenz fürchteten, werden 2017 eher Umsatzzuwächse erwartet. Inhaltlich ist einerseits weniger Unsicherheit zu erkennen, auf der anderen Seite sind die Erwartungen in vielen Bereichen negativer geworden: es wird weniger Rechtssicherheit erwartet, die Positionen der DSB werden eher als geschwächt wahrgenommen. Allerdings fand die Befragung vor den Entscheidungen zum neuen BDSG statt, die sicher weitere Meinungsumschwünge hervorgerufen haben dürfte.

Mitgliederbefragung – Während der Übergangszeit der DS-GVO erwarte ich für mich/uns...



Mitgliederbefragung – Von der DS-GVO erwarte ich persönlich:



Mitgliederbefragung Zusammenfassung

- In vielen Bereichen positive bewertete Arbeit: Seminare, Geschäftsstelle, Öffentlichkeit
- Nachholbedarf bei Arbeitshilfen
- Einige Angebote müssen bekannter werden

Über den Autor



Dr. Kai-Uwe Loser

Diplom-Informatiker, Dr. rer. nat. (Universität Dortmund), geprüfter Datenschutzauditor (TÜV)

Besteller behördlicher Datenschutzbeauftragter der Ruhr-Universität Bochum
 Besteller behördlicher Datenschutzbeauftragter der Universität Duisburg-Essen
 Vorstand im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

»MIT DEN JAHREN WIRD SIE IMMER JÜNGER.«

Die BvD-News feiert im August ihren 20. Geburtstag als Mitgliedermagazin.

Neue Internetseite, neue Verbandszeitschrift: Was aktuell klingt, liegt 20 Jahre zurück. Im August 1997 erschien die BvD-News das erste Mal als offizielle Verbandszeitschrift des BvD.

Damals waren gerade vier neue Vorstandsmitglieder ins Team um BvD-Vorsitzenden Professor Gerhard Kongehl gekommen: Alwin Baumeister, Holger Heimann, Helmut Franz und Markus Mix. Mit Engagement und frischem Enthusiasmus ging es an die Öffentlichkeitsarbeit. Eine neue Website entstand – und die BvD-News sollte von da an mindestens drei Mal im Jahr erscheinen.

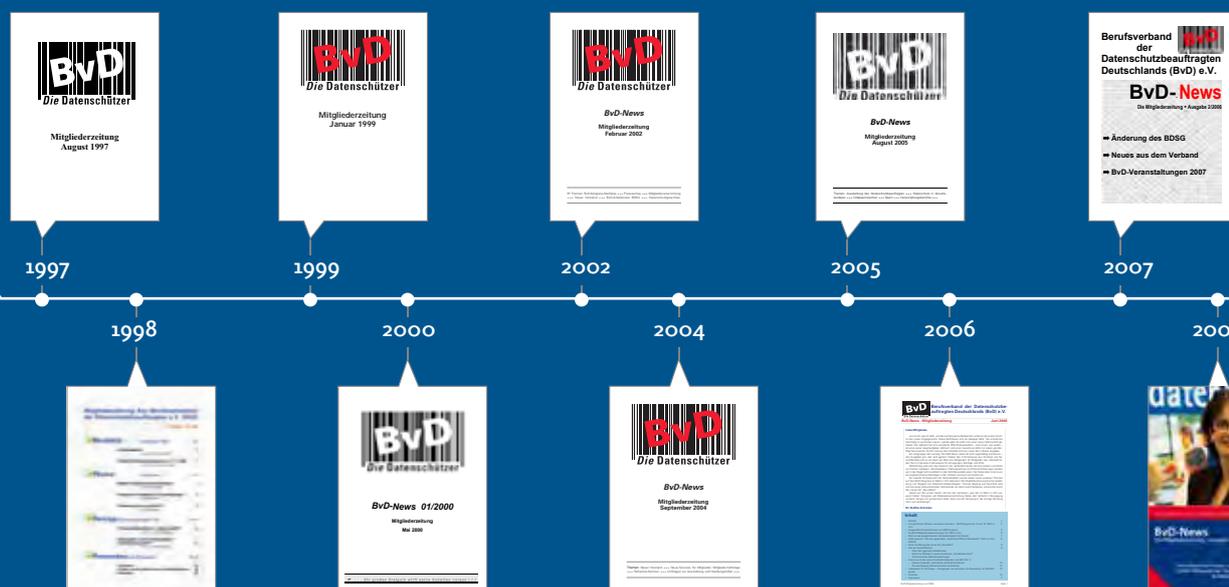
»Die Themen der ersten Ausgabe beschäftigen uns auch heute noch«, sagt der jetzige BvD-Vorstandsvorsitzende Thomas Spaeing. Schon in der ersten Ausgabe ging es um Verschlüsselungsverfahren, um die Rolle der betrieblichen Datenschutzbeauftrag-

ten in Unternehmen – und um ein neues Gesetz für Datenschutz. »1997 war stark von der Diskussion um die geplante Novelle des Bundesdatenschutzgesetzes geprägt«, erinnert sich Thomas Spaeing. »Das war damals mindestens so ein Einschnitt wie heute die Datenschutz-Grundverordnung.«

Der frischgeklärte Vorstand Markus Mix erklärte den BvD-Mitgliedern in einem Beitrag, was eine Firewall ist – damals eines der neuen Themen zur Sicherheit von Unternehmensdaten. Denn erst wenige Jahre zuvor hatten Hacker die Internet-Kommunikation mehrere US-Behörden und Universitäten angegriffen, die damals das weltweite Netz dominierten. Seine Erläuterungen zu Abwehrkonzepten wie Paketfilter, Proxy Servern und Circuit Level Gateways sind auch heute noch lesenswert.

BvD-News – im Wandel der Zeit

20 JAHRE
BvD-News



Noch gut erinnert sich Thomas Spaeing an das damalige Logo, das den Titel der ersten BvD-news zierte: BvD als roter Schriftzug auf einem schwarz-weißen Strichcode. »Die Idee dafür hatten die Vorstandsmitglieder selbst entwickelt«, erinnert sich Spaeing. Heute sitzen Text- und Gestaltungsprofis an den aktuellen Ausgaben.

Mit dem neuen Logo 2010 erhielt auch die BvD-News ein Lifting: Die Titel wurden frischer, das Heft umfangreicher. In den vergangenen Jahren erhielt sie außerdem eine Rubriken-Struktur und mehr Seiten. »Wir sind als Verband gewachsen, und das sieht man auch der BvD-News an«, sagt Thomas Spaeing. »Aber ich finde: Mit den Jahren wird sie immer jünger.«

Die BvD-News heute

Fachautoren aus der Datenschutz-Praxis, aber auch Aufsichtsbehörden und Politiker stellen ihre Standpunkte zum Datenschutz und zu den Aufgaben von Datenschutzbeauftragten in exklusiven Fachartikeln dar und liefern topaktuelle und wichtige Informationen, Empfehlungen und Tipps.

- Zielgruppe:** behördliche und betriebliche Datenschutzbeauftragte, Datenschutz- und Datenschutzsicherheitsfachleute, IT-Fachleute, Juristen, Personal und Betriebsräte
- Druckauflage:** 2.500 Exemplare
- Verbreitete Auflage:** 2.300 Exemplare
- Erscheinungsweise:** 2 x jährlich, plus Sonderausgabe
- Zeitungsformat:** 210 x 297 mm
- Papier:** 250 g Umschlag / 115 g Inhalt, BD matt
- Farbigkeit:** 4-farbig / CMYK
- Seitenumfang:** zw. 68 und 86

Online abrufbar unter:
www.bvdnet.de/bvd-news/



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

Unsere nächsten Treffen der Arbeitskreise und Regionalgruppen:

11./12.08.2017	AK Arbeitshilfen	20.10.2017	RG Nürnberg
12.09.2017	RG Ost	27.10.2017	RG München
21.09.2017	AK Sozial	06.11.2017	RG Ost
22./23.09.2017	AK Externe	09./10.11.2017	AK Medizin
28.09.2017	RG Mitte	16.11.2017	AK EVU
06.10.2017	RG Karlsruhe	27.11.2017	AK Krypto
18.10.2017	AK Schule	01.12.2017	AK Finanzdienstleistung
20.10.2017	RG Ulm		

BvD-VERBANDSTAG(E)

Save the Date

Die Termine für die nächsten BvD-Verbandstage stehen fest.

Bitte schon jetzt vormerken.

- ▶ <https://www.bvdnet.de/bvd-verbandstag/>

BvD-Verbandstage 2018: 25./26.04.2018

BvD-Verbandstage 2019: 05./06.06.2019

BvD-Verbandstage 2020: 06./07.05.2020

Überblick

Seminare und Workshops

ab September 2017



ab
399,-- €
 zzgl. MwSt. *

Termin	Seminar/ Workshop	Ort
19.09.2017	Neue Herausforderungen & Aufgaben sowie Haftung des DSB in der DS-GVO	NH Düsseldorf Nord Referent: Stefan Sander
21.09.2017	Datenschutz-Compliance nach der DS-GVO	NH Collection Nürnberg Referent: Andreas Sachs, Markus Gierschmann
23.10.2017	Auftragsverarbeitung BDSG – DS-GVO	NH Hotel Berlin Mitte Referent: Dr. Christoph Bausewein
24.10.2017	Praxisworkshop Auftragsdatenverarbeitung	NH Hotel Berlin Mitte Referenten: Dr. Christoph Bausewein/ Jürgen Hartz
06.11.2017	Die ePrivacy-Verordnung – Ergänzung zur DS-GVO	NH Düsseldorf Nord Referent: Kristin Benedikt
21.11.2017	Dokumentation nach DS-GVO im Sinne der Rechenschaftspflicht	NH Düsseldorf Nord Referent: Bernd Fuhlert
22.11.2017	Umsetzung des risikobasierten Ansatzes der DS-GVO in der Praxis	NH Düsseldorf Nord Referent: Stephan Rehfeld

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.



Mehr Sicherheit für Ihre vertraulichen Daten.

www.folderflex.de

Marketing

FÜR DEN BESTEN
EINDRUCK
www.tpdigitaldruck.de

 **Trend Point Marketing GmbH**
Salzufer 15/16 (Gebäude D) | 10587 Berlin

Datenschutz

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

**Jetzt informieren
unter www.udis.de**



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*

Auditierung

DSZ **DATENSCHUTZ**
Zertifizierungsgesellschaft mbH
EIN UNTERNEHMEN
VON GDD UND BVD

Datenschutz Zertifizierung:
unabhängig – transparent – standard-basiert

www.dsz-audit.de

Treffen Sie Entscheider aus Kundendienst & Service

Jetzt kostenlos Mitglied werden im KVD e. V.*



- **Datenschutz und mehr:** Im KVD sind europaweit mehr als 1.600 Fach- und Führungskräfte aus dem direkten Kundendienst und der Service-Industrie engagiert
 - **Experten- und Kompetenzgruppen** der Dienstleistungswirtschaft halten Sie „up to date“ zu den relevanten Themen in den Bereichen Mensch, Prozess und Technologie
 - **EXKLUSIVE Veranstaltungen für KVD-Mitglieder bei Deutschlands führenden Dienstleistern in Sachen Datenverarbeitung:** Die Event-Reihe „Service goes live“ – unter anderem bei der Samhammer AG, DIN e. V., DHL, dtms, arvato services, IBM Service Center, UPS und SAP – ist für Mitglieder kostenfrei
 - Mit dem jährlichen Service Congress und den regelmäßigen Fachtagungen zu Personalfragen im Service erleben Sie neben den exklusiven Betriebsbesichtigungen die **Service-Praxis hautnah**
 - Der „**Marktplatz**“ für **innovative Lösungen** und exzellente Services unterstützt Sie in der täglichen Praxis, wenn es um Kundendialog, Service-Marketing, Kundenpflege und -akquise oder auch den datenschutzkonformen Einsatz von CRM- und weiteren Kundenmanagement-Systemen geht.
- * **Unsere besondere Aktion für BvD-News-Leser: Melden Sie sich mit dem Stichwort BvD2017 als neues Mitglied an – und Sie erhalten eine kostenfreie Probemitgliedschaft bis zum 31.12.2017 mit allen genannten Leistungen.**

Zum Ende der Probemitgliedschaft entscheiden Sie, ob Sie weiter KVD-Mitglied bleiben möchten. Und so geht's: Melden Sie sich in der KVD-Geschäftsstelle unter Tel: 02362 . 9873-0 oder füllen Sie auf www.kvd.de den Mitgliedsantrag aus – alles andere erledigen wir für Sie!



Infos & Anmeldung unter www.kvd.de

QR-Code mit Ihrem Smartphone einscannen und direkt zur Mitgliederinfo gelangen.

Datenschutz im Fokus.



ZD – Zeitschrift für Datenschutz

7. Jahrgang 2017. Erscheint monatlich mit 14-täglichem Newsdienst ZD-Aktuell und Online-Modul ZDDirekt.

Jahresabonnement € 235,-

Vorzugspreis für BvD-Mitglieder,

für Abonnenten der Zeitschrift MMR und des beck-online Moduls IT- und Multimediarecht PLUS sowie für ausgewählte Kooperationspartner € 175,-. Vorzugspreis für Studenten und Referendare € 109,-

Abbestellung bis 6 Wochen vor Jahresende. Preise jeweils inkl. MwSt. zzgl. Vertriebs-/Direktbeorderungsgebühren Inland (€ 13,30/€ 2,80) € 16,10 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.