Ausgabe 03/2017

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Save the Date!
BvD-Verbandstage
25.04./26.04.2018
im ELLINGTON HOTEL BERLIN
Nürnberger Str. 50-55,
10789 Berlin

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Das Bundesdatenschutzgesetz 2018: Herausforderungen für die Datenschutzpraxis

EIN NEUES FORMAT FÜR DEN DATENSCHUTZ – ab S. 5

BESCHÄFTIGTENDATENSCHUTZ NACH DEM NEUEN BDSG – ab S. 32

DS-GVO LEGT FOKUS AUF DATENSICHERHEIT – ab S. 58

„DATENSCHUTZ GEHT ZUR SCHULE“ – ab S. 87

BvD e.V.
DATENSCHUTZ GESTALTEN

Anzeige

Jetzt anmelden unter:
www.bvdnet.de/bvdverbandstag

BvD e.V.
DATENSCHUTZ GESTALTEN

2018

BvD-Verbandstage | 25.04./26.04.2018

im ELLINGTON HOTEL BERLIN
Nürnberger Str. 50-55, 10789 Berlin

Verleihung Datenschutz Medienpreis des BvD (DAME)
am 25.04.2018 zur Abendveranstaltung

»BvD-Verbandstage 2018 –
Wegweisend im Datenschutz«

u. a. mit folgenden Themen:

- Umsetzung der DS-GVO in Unternehmen
- Privacy by design/by default – Anforderungskriterien aus Kundensicht
- Datenschutz-Compliance
- Beschäftigtendatenschutz
- Einwilligung

WIRTSCHAFT TRIFFT AUFSICHT – POLITIK TRIFFT NICHT!

Rund 200 Teilnehmer besuchen die erste Herbstkonferenz des Landesdatenschutzbeauftragten Baden-Württemberg und des BvD in Stuttgart. Der Digitalpolitik hingegen fehlen die Konzepte.

Liebe Leserinnen und Leser,

die Datenschutzaufsichtsbehörden der Länder stehen bereit, um Unternehmen und Behörden zu den neuen datenschutzrechtlichen Anforderungen zu beraten. Insofern besteht der Anspruch – wie auch bisher – als Ansprechpartner auch schon bei der Planung neuer Verarbeitungen wahrgenommen zu werden und die Unternehmen dabei zu unterstützen, die neuen gesetzlichen Anforderungen angemessen zu berücksichtigen. Während der „Herbstkonferenz Datenschutz" in Stuttgart, die der Landesdatenschutzbeauftragte Baden-Württemberg, Herr Dr. Brink, und der BvD gemeinsam veranstaltet haben, wurde klar, dass dabei noch viel Diskussionsbedarf besteht, da viele Regelungen insbesondere der DS-GVO noch nicht so ausgelegt sind, dass Klarheit über den besten Lösungsansatz besteht.

Auf jeden Fall hat der Kongress gezeigt, dass Wirtschaft und Aufsichtsbehörden hier an einem Strang ziehen möchten, um die Regelungen in angemessener Form umsetzen zu können.

Und was macht die Politik mit dem neuen Datenschutzrecht?

Wenn man sich die politische Diskussion zum Datenschutz anschaut, dann gewinnt man leider den Eindruck, dass viele Akteure das Potential des Themas immer noch nicht erkannt haben. Da werden „Datengesetze" im Verkehrsministerium entwickelt, die völlig losgelöst vom geltenden Datenschutzrecht und der bisherigen Linie beim Datenschutz in Europa vor allem Lobbyinteressen berücksichtigen.

Förderprogramme für innovative technische Lösungen zur Umsetzung des neuen Datenschutzrechts, die sich zu weltweiten Exportschlagern entwickeln könnten: Fehlanzeige. Diese Lösungen kommen dann wieder aus Asien oder den USA. Der deutschen Politik fehlt es hier wieder an der dringend gebotenen Weitsicht.

Und die Digitalpolitik?

Um den digitalen Wildwuchs in der Politik zu beenden, soll es nun einen neuen Ansprechpartner für Digitales geben – Super, endlich! Aber: Bitte nur einen! Nicht dieses Kompetenz-Wirrwarr wie bisher. Ob das dann ein Ministerium oder ein Staatsminister im Kanzleramt wird, ist vollkommen egal. Einen Praktiker, der sich hier auskennt, darauf käme es an. Aber leider funktioniert die Politik in Deutschland schon lange nicht mehr so.

Um gleich noch ein weiteres wichtiges Tätigkeitsfeld anzusprechen: Wenn wir bei der Digitalisierung aufholen wollen, im weltweiten Vergleich, dann müssen endlich auch die passenden Bildungskonzepte und Lehrerausbildungen her – auch erfahrene Praktiker sollten dabei eingebunden werden! Wenn aber die Schüler hierzulande den Informatikunterricht nur als verschlafenes Thema bei einem völlig überforderten Lehrer erfahren, darf es uns nicht wundern, dass wir sie später für dieses Thema nicht mehr begeistern können. In der Folge fehlen uns die Fachkräfte für die digitale Aufholjagd, die damit wohl eher mager ausfallen dürfte. Das ist heute die bittere Realität.

Wie auch immer die nächste Regierung in Deutschland aussieht, hier gibt es für die Zukunft des Landes viel zu tun.

Ich wünsche Ihnen eine anregende Lektüre.

T. Spaeing

Thomas Spaeing

BvD-Vorstandsvorsitzende

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

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

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

Fotos:
123rf.com

Lektorat:
Frank Spaeing

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

Satz und Layout:
Trend Point Marketing GmbH,
Salzufer 15/16, 10587 Berlin
www.tpmarketing.de

Druck:
Trend Point Marketing GmbH,
Salzufer 15/16, 10587 Berlin
www.tpmarketing.de

ISSN: 2194-1025
Erscheinungsweise: 3 × 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 gekennzeichnete Beiträge müssen nicht die Meinung des BvD e.V. wiedergeben.

EDITORIAL

Editorial: Wirtschaft trifft Aufsicht – Politik trifft nicht! – *Thomas Spaeing* 3

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Ein neues Format für den Datenschutz – *BvD-Herbstkonferenz Datenschutz* 5
Von der Artikel-29-Gruppe zum Europäischen Datenschutzausschuss (EDSA) – Zukunft und Bedeutung der Working Papers – *Alexander Filip* 8
Herausforderung „EU-Datenschutz-Grundverordnung" – Die Kunst der erfolgreichen Umsetzung – *Detlef Klett, Mareike Gehrmann, Julian Klett* 13
Checklisten als Hilfsmittel zur Umsetzung der DS-GVO – *Michael Punz* 18
Konzerndatenschutz in der DS-GVO – praktische Umsetzung in einer Unternehmensgruppe – *Timo Ahland* 22
Auftragsverarbeiterhaftung nach der DS-GVO - Was ändert sich in der Praxis? – *Thomas Kahl* 27
Beschäftigtendatenschutz nach dem neuen BDSG – *Tim Wybitul und Kai Wendt* 32
Sicherheit der Verarbeitung nach der Europäischen Datenschutzgrundverordnung. Was ändert sich, was bleibt? – *Helmut Eiermann* 37
Vorgehen bei Datenschutz-Folgenabschätzungen – *Dr. Michael Friedewald und Dr. Nicholas Martin* 41
Recht auf Löschung: Der Radiergummi der DS-GVO – *Tilman M. Dralle, LL.M.* 46
Unterschreiten des Stands der Technik – *Rechtsanwalt Karsten U. Bartels LL.M.* 50

DATENSCHUTZPRAXIS

Datenschutz-Zertifizierung nach dem Trusted Cloud Datenschutz-Profil für Cloud Dienste – *Sascha Adler* 54
DS-GVO legt Fokus auf Datensicherheit – *Christian Volkmer* 58
Dienstleister im Gesundheitswesen – *Barbara Stöferle* 62
Der aktuelle Gesetzesentwurf zum neuen Schweizer Datenschutzrecht (VE-DSG-CH) – *Marcel Griesinger und Jutta Sonja Oberlin* 68
Die vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln als Hemmschuh der E-Mail-Verschlüsselung – ein Lösungsansatz – *Stephan Blazy, Susan Gonscherowski, Thomas Kunz, Annika Selzer, Ulrich Waldmann* 72
Spät, aber noch nicht zu spät – *Evelyn Seiffert* 76

AUFSICHTSBEHÖRDE

„Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht" – *Handreichung des Hessischen Datenschutzbeauftragten* 79

AUS DEM VERBAND

Zertifizierung – Ein Zwischenstand – *Dr. Niels Lepperhoff* 83
Gutachten des BvD zu Stellung, Pflichten und Haftung des DSB in der DS-GVO – *Konrad Menz* 84
Schulungskonzept des AK Arbeitshilfen – *Regina Mühlich / Prof. Bernd Beier* 86
„Datenschutz geht zur Schule" im Kaiserbahnhof – *Ralf Heimburger* 87
Neue Runde beim Nürnberger Daten-Dienstag 89
BvD befragt Unternehmen zum Start der DS-GVO im Mai 2018 90

REZENSIONEN

Sassenberg / Faber; Rechtshandbuch Industrie 4.0 und Internet of Things 91
Lepperhoff, Dr. Niels / Müthlein, Thomas; Leitfaden zur Datenschutz-Grundverordnung 92
Schneider, Jochen; Datenschutz nach der EU-Datenschutz-Grundverordnung 93
Stiftung Datenschutz (Hrsg.); Band 2 der Reihe Daten Debatten „Big Data und E-Health" 94
Gernot Syrow (Hrsg.); Europäische Datenschutzgrundverordnung Handkommentar 95

TERMINE

Termine der Regionalgruppen und Arbeitskreise des BvD 96
Überblick Seminare und Workshops 2017/2018 97

SERVICE

Wichtige Kontakte im Überblick 98

EIN NEUES FORMAT FÜR DEN DATENSCHUTZ

Der BvD und der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg luden erstmals zur gemeinsamen Herbstkonferenz.

Unter dem Motto „Wirtschaft trifft Aufsicht" initiierten BvD und LfDI BaWü am 26. und 27. Oktober in Stuttgart die erste Herbstkonferenz überhaupt – mit überwältigendem Erfolg. 200 Teilnehmende diskutierten mit Vertretern und Kollegen von Aufsichtsbehörden aus Deutschland, Österreich, Liechtenstein und der Schweiz über die Vorbereitungen auf den 25. Mai 2018.

Im Zentrum des zweitägigen Austauschs stand die Frage, wie sich Unternehmen gerade auch mit grenzüberschreitender Datenverarbeitung auf den Wechsel zur DS-GVO vorbereiten – und welche Unterstützung sie benötigen. Unter anderem sprachen Staatssekretär Martin Jäger aus dem Baden-Württembergischen Innenministerium und Thomas Kranig, Präsident des Bayerischen Landesamts für Datenaufsicht.

Schon jetzt ist klar: Auch 2018 wird es neben dem BvD-Verbandstag in Berlin wieder eine Herbstkonferenz in Kooperation mit der Baden-Württembergischen Aufsichtsbehörde geben. Thomas Kranig kündigte bereits an, die nächste Konferenz als Mitausrichter mit unterstützen zu wollen.

Nur 15 bis 20 Prozent der Betriebe dürften die Vorgaben zum Stichtag erfüllen

Schnell stellte sich in Stuttgart heraus: Die Mehrzahl der Unternehmen in Deutschland ist bislang nicht ausreichend auf die Änderungen vorbereitet, die die DS-GVO zum 25. Mai 2018 verlangt. *„Nur 15 bis 20 Prozent dürften die Vorgaben zum Stichtag erfüllen"*, schätzt Baden-Württembergs oberster Datenschützer Stefan Brink. Das sei aber nicht so schlimm, beruhigt er. Denn viele Unternehmen seien auf einem guten Weg.

Vor allem große Firmen und Konzerne, die bereits in der Vergangenheit ein ausgeprägtes Datenschutzregime aufgebaut hatten, sehen sich für den Paradigmenwechsel gewappnet. Die Daimler AG in Stuttgart beispielsweise hat 28 Arbeitspakete definiert, die nach und nach umgesetzt werden, erläutert Joachim Rieß, Rechtsanwalt und Konzerndatenschutzbeauftragter bei der Daimler AG in Stuttgart.

Alles kann nicht bis zum 25. Mai umgesetzt werden, betont Rieß. Dazu gehört beispielsweise auch die Umsetzung Datenschutz-Folgenabschätzung und der Löschkonzepte. Er geht davon aus, dass der Konzern zwei Drittel der Arbeitspakete bis Mai 2018 umsetzt, *„die anderen müssen wir fortlaufend implementieren"*.

Bei der Unternehmensgruppe Procter & Gamble Deutschland sieht es ähnlich aus. Die Grundphase sei abgeschlossen, jetzt versuche der Konzern die Hauptpunkte zum Beispiel im Consumer-Bereich bis zum 25. Mai zu etablieren, sagt Jörg Becker, Datenschutzbeauftragter des Konzerns in Deutschland. Die übrigen Punkte müssten dann nach und nach umgesetzt werden.

„Vieles wird uns selbst erst nach und nach klar", sagt er. Niemand habe Erfahrung mit den neuen Verfahren, wie viel Zeit auf welche Aufgabe entfalle und wie viel Personen dafür eingeplant werden müssten.

Procter & Gamble Deutschland hat für die Umstellung auf die DS-GVO ein Team aufgebaut, zur Umsetzung würden Mitarbeiter speziell im Datenschutz trainiert und ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

in regionale Datenschutz-Teams aufgenommen. *„Die Umstellung ist bei uns Chefsache und wird von den Vorständen für Deutschland, Österreich und Schweiz unterstützt."*

Das ist nicht überall so. Von allen Unternehmen, die er als externer Datenschützer berät, habe er nur bei einem die uneingeschränkte Rückendeckung der Geschäftsführung, berichtet Ulrich Ilgner von dem Ulmer Sicherheitsunternehmen ditis. Er beobachtet eine mangelnde Bereitschaft bei Unternehmen, sich mit den Anforderungen der DS-GVO auseinanderzusetzen. Entsprechend würden kaum Ressourcen zur Vorbereitung zur Verfügung gestellt. *„Nur in einem Unternehmen gibt es eine Assistentin für das Thema, bei allen anderen bin ich Einzelkämpfer"*, sagt Ilgner. Es sei aber die Aufgabe von Geschäftsführern, sich dieser Verantwortung zu stellen.

Ilgner kann deshalb Kontrollen und Bußgeldern nach dem 25. Mai 2018 auch etwas Positives abgewinnen: *„Ich hoffe, dass das Verhängen von Bußgeldern auch in den Medien publiziert wird um das Bewusstsein für den Datenschutz und die DS-GVO zu schärfen."*

Europaweite gleichmäßige Auslegung

Die Aufsichtsbehörden selbst sehen die Situation nicht ganz so negativ. Viele Unternehmen hätten sich auf den Weg gemacht, bräuchten aber noch etwas länger, erläutert Baden-Württembergs oberster Datenschützer Stefan Brink. *„Wenn wir bei Kontrollen feststellen, ein Unternehmen hat das Problem erkannt und ist dabei, umzustellen, braucht aber vielleicht noch drei oder sechs Monate länger, dann ist das besser, als wenn ein Unternehmen sich mit den neuen Anforderungen überhaupt nicht auseinandersetzt"*, sagt er.

Unternehmen, die das Thema ignorierten, müssten mit Bußgeldern rechnen. *„Das verlangt das Gesetz"*, sagt Brink. Vor allem müsse die Verordnung europaweit gleichmäßig ausgelegt werden.

Er geht davon aus, dass die französischen und spanischen Behörden früh Kontrollen durchführen und Bußgelder verhängen werden. *„Dann ist es nicht nur eine Frage der Fairness, dass wir in Deutschland auch zügig Kontrollen durchführen"*, sagt er. Es gehe vielmehr um den gleichmäßigen Vollzug der europäischen Rechtsgrundlage. *„Wir können in Deutschland keinen Rabatt geben oder uns zurückhalten. Da stehen wir selbst unter Druck"*, sagt Brink.

Um die Unternehmen bei der DS-GVO zu unterstützen, bietet die Aufsichtsbehörde Vorträge, Arbeits- und Auslegungshilfen und auch branchenspezifische Unterstützung an.

Brink räumt ein, dass die Aufsichtsbehörden schon etwas früher hätten loslegen können. Sein Haus biete seit Sommer 2017 allgemeine Beratung und Unterstützung an. *„Vielleicht hätten wir direkt im Sommer 2016 losmarschieren sollen"*, sagt Brink. *„Da müssen wir uns auch an die eigene Nase fassen."*

„Wir müssen Ernst machen"

Barbara Thiel, Landesbeauftragte für den Datenschutz Niedersachsen, hat Anfang November ein Informationspapier herausgegeben, in dem sie vor allem kleine und mittlere Unternehmen auf die Dringlichkeit der Umstellung hinweist. *„Wir stehen beratend zur Verfügung. Auf meiner Homepage finden sich die unterschiedlichsten Informationen. Und die vielen Vorträge, die ich halte, zeigen, wie groß der Unterstützungsbedarf bei den Unternehmen ist"*, sagt sie.

Thiel schätzt, dass sich vor allem kleine und mittlere Unternehmen noch gar nicht mit der neuen DS-GVO auseinandergesetzt haben. Mit den Kammern in Niedersachsen ist sie deshalb seit geraumer Zeit im Gespräch, um Informationsveranstaltungen durchzuführen, auf denen erläutert wird, welche Anforderungen die DS-GVO an die Unternehmen stellt.

Thiel ist fest entschlossen, nach dem 25. Mai 2018 mit den Kontrollen zu beginnen. *„Wir müssen Ernst machen"*, sagt sie. Die Drohkulisse mit Sanktionen könne nur funktionieren, wenn die Aufsichtsbehörden tatsächlich nachprüften, welche Punkte die Unternehmen umgesetzt hätten. *„Das Datenschutzrecht ist letztendlich nur so gut, wie es vollzogen und durchgesetzt wird"*, sagt sie.

Auch in der Vergangenheit seien Kontrollen betrieben worden, sagt Thiel. *„Jetzt haben wir aber einen deutlich erweiterten Auftrag."* Sie hofft, dass ihre Behörde im Frühjahr 2018 über die die ersten Prüfkonzepte verfügt, die derzeit in ihrem Hause entwickelt werden.

„Mittendrin und voll dabei"

Solche Hilfen sind dringend nötig, mahnt BvD-Vorstandsmitglied Jens Eckhardt an. *„Die Anforderungen der DS-GVO sind kompliziert, wenig praxisnah und selbst wenn man nur Einzelregelungen betrachtet, kommt man schnell zur Frage: Was bedeutet das eigentlich"*, kritisiert der Jurist. Der BvD hat deshalb eine Reihe von Auslegungshilfen, Checklisten und weitere Unterlagen zur Unterstützung bei der Umstellung aufgelegt.

Doch selbst mit Hilfe der Leitfäden könnten für Unternehmen keine eindeutigen Verfahrensprozesse entwickelt werden, sagt Eckhardt. *„Die Unternehmen überlegen sich sehr wohl, ob sie ein Verfahren aufsetzen, von dem sich später vielleicht herausstellt, dass man es viel einfacher und kostengünstiger regeln kann"*, sagt er.

Allerdings seien viele Unternehmen seiner Erfahrung nach auch gut aufgestellt, andere seien jetzt an dem Punkt, an dem sie einsähen, dass es nicht einfacher wird. Deshalb versuchten sie umzusetzen, was zum 25. Mai 2018 möglich ist. *„Wir sind mittendrin und voll dabei"*, sagt Eckhardt.

Herbsttagung 2018 mit Aufsichtsbehörden aus Bayern und Baden-Württemberg

Um Unternehmen in diesem intensiven Prozess weiterhin zu begleiten, wird der BvD regelmäßig weitere Arbeitshilfen zur Verfügung stellen. Direkt vor der Umstellung lädt der BvD am 25. und 26. April zu seiner Jahrestagung 2018 nach Berlin ein. Er wird unter anderem ein Resümee der bis dato erfolgten Vorbereitungen ziehen.

Die Herbstkonferenz 2018 vom 24.10.-26.10.2018 in Stuttgart legt dann den Fokus auf den Stand der Umsetzungen nach dem Stichtag 25. Mai. Der 26.10. wird auf Vorschlag von Dr. Stefan Brink und Thomas Kranig thematisch auf die Belange der Behörden und Öffentlichen Stellen sowie deren DSB ausgerichtet. Die zweite Ausgabe des neuen Formats wird wieder vom BvD in enger Kooperation mit Baden-Württembergs Landesdatenschutzbeauftragten, Stefan Brink, und – als neuem Partner – voraussichtlich von Thomas Kranig als Präsident des Bayerischen Landesamts für Datenaufsicht gemeinsam initiiert.

Stefan Brink fand zum Abschluss der ersten Herbstkonferenz in Stuttgart nur lobende Worte: Er habe *„viel positive Resonanz"* auf die Tagung, ihre Organisation und inhaltliche Vorbereitung erhalten. Das habe ihn schnell dazu bewogen, das Format mit dem BvD weiterzuführen, sagte er unter großem Applaus zum Abschluss.

Alle Informationen zur BvD-Herbstkonferenz Datenschutz inkl. aller bereitgestellten Vorträge finden Sie auf unserer Webseite unter:

https://www.bvdnet.de/termin/herbstkonferenz-zum-datenschutz/.

Über die Autorinnen

Katrin Eggert (Interviews)
BvD-News Redaktion

Christina Denz (Text)
freie Journalistin

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

VON DER ARTIKEL-29-GRUPPE ZUM EUROPÄISCHEN DATENSCHUTZ-AUSSCHUSS (EDSA) – ZUKUNFT UND BEDEUTUNG DER WORKING PAPERS

Alexander Filip

Die Europäische Datenschutz-Grundverordnung (DS-GVO), die ab dem 25. Mai 2018 anwendbar sein wird und die EG-Datenschutzrichtlinie (Richtlinie 95/46/EG; nachfolgend: EG-DSRL) aus dem Jahr 1995 ablöst, verfolgt das Ziel einer grundsätzlich umfassenden Harmonierung des Datenschutzrechts in der EU (vgl. Selmayr/Ehmann, DS-GVO, Kommentar, 2017, Einführung, Rn. 79). Die Wahl einer Verordnung als Gesetzgebungsinstrument spiegelt dieses Ziel des Gesetzgebers wider: Eine europäische Verordnung hat gemäß Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) unmittelbare Geltung und bedarf – außer dort, wo sie den EU-Mitgliedstaaten ausdrücklich noch Spielräume zur Konkretisierung und Spezifizierung belässt – keiner weiteren Umsetzung durch den nationalen Gesetzgeber. Das Ziel der EU-weiten Harmonisierung des Datenschutzrechts wird in mehreren Erwägungsgründen der DS-GVO auch ausdrücklich angesprochen, etwa in ErwGr 10, wonach die Verordnung ein „gleichmäßiges und hohes Datenschutzniveau" in der EU gewährleisten soll. Im Übrigen dürfen die Mitgliedstaaten selbst dort, wo ihnen die DS-GVO Spielräume zur Spezifizierung und Konkretisierung belässt, dabei nicht von dem Schutzniveau der DS-GVO abweichen: Eine Absenkung des Schutzniveaus wäre mit dem europarechtlichen Grundrecht auf Schutz personenbezogener Daten (Art. 8 EU-Grundrechtecharta) nicht vereinbar, während eine Erhöhung des durch die DS-GVO gewährleisteten Schutzniveaus durch nationales Recht dem durch die DS-GVO gleichfalls vorgegebenen Ziel des freien Verkehrs personenbezogener Daten in der EU (Art. 1 Abs. 3 DS-GVO) zuwiderliefe (Selmayr/Ehmann, wie oben, Rn. 89).

Die vom Gesetzgeber beabsichtigte Einheitlichkeit des Datenschutzniveaus in der EU erfordert neben der Einheitlichkeit der Rechtsvorschriften auch deren unionsweit einheitliche Anwendung. Eine entscheidende Rolle kommt in diesem Zusammenhang dem Europäischen Datenschutzausschuss (EDSA) zu. Der EDSA wird durch die DS-GVO als Einrichtung der Europäischen Union mit eigener Rechtspersönlichkeit eingerichtet und besteht aus den Leitern der Datenschutzaufsichtsbehörden aller EU-Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten bzw. ihren jeweiligen Vertretern (Art. 68 DS-GVO). Der EDSA ist - oberflächlich betrachtet - Nachfolgeeinrichtung der durch die EG-DSRL von 1995 eingeführten so genannten Artikel-29-Gruppe, allerdings ist er mit ungleich weitreichenderen Aufgaben und Befugnissen als die Art.-29-Gruppe ausgestattet. Der Art.-29-Gruppe kam lediglich eine beratende Funktion zu: Sie konnte nicht-bindende Empfehlungen und Stellungnahmen zu grundsätzlich allen datenschutzrechtlichen Fragen in der EG abgeben (siehe Art. 29 Abs. 1 UAbs. 2 sowie Art. 30 EG-DSRL). In diesem Rahmen hat die Art.-29-Gruppe seit ihrem Bestehen eine Vielzahl an Stellungnahmen zur Auslegung und Anwendung des europäischen Datenschutzrechts und insbesondere zur EG-Datenschutzrichtlinie abgegeben, allen voran über 240 so genannte Arbeitspapiere („Working Papers"; kurz: WP), darunter „Stellungnahmen" (engl.: opinions), „Erklärungen" (engl.: statements) und „Arbeitsdokumente" (engl.: working documents). Neben diesen Arbeitspapieren hat die Gruppe noch weitere Äußerungen veröffentlicht, z.B. in der Form von Briefen (engl.: letters) an verschiedene Institutionen oder auch Unternehmen. Die von der Art.-29-Gruppe veröffentlichten Papiere sind online unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm sowie http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 abrufbar (diese Zweiteilung ist der derzeit stattfindenden Überarbeitung der Internet-Präsenz der Artikel-29-Gruppe geschuldet).

Viele Unternehmen und andere Rechtsanwender haben die zahlreichen Veröffentlichungen der Art.-29-Gruppe in den letzten Jahren aufmerksam verfolgt. Gerade für international tätige Unternehmensgruppen mit Aktivitäten in mehreren EU-Mitgliedstaaten waren und sind die Arbeitspapiere der Art.-29-Gruppe eine wertvolle Auslegungs- und Anwendungshilfe zur EG-DSRL. Sie haben zudem den Vorteil, den Unternehmen und anderen Anwendern aufzuzeigen, wie die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten die EG-DSRL mehrheitlich interpretieren und ihnen somit vor Augen zu führen, in welchen Fällen ein bestimmtes Vorgehen zu „Problemen mit der Aufsichtsbehörde" führen könnte. In der von zahlreichen Auslegungsfragen und der daraus folgenden gewissen Rechtsunsicherheit geprägten Materie des Datenschutzrechts waren die Arbeitspapiere der Art.-29-Gruppe deshalb ein wichtiges Element zur Stärkung der Rechtssicherheit – selbst wenn sie natürlich bei weitem nicht alle Fragen zur Interpretation der EG-DSRL abschließend klären konnten.

Die Art.-29-Gruppe traf und trifft ihre Entscheidungen mit der Mehrheit der abgegebenen gültigen Stimmen (Art. 12 Abs. 1 der Geschäftsordnung / rules of procedure der Artikel-29- Gruppe; online auf der zweitgenannten der o.g. beiden Websites abrufbar). Auch wenn die Arbeitspapiere der Art.-29-Gruppe somit nicht notwendigerweise immer die Position aller einzelnen Datenschutzaufsichtsbehörden in der EU zu einer bestimmten Frage widerspiegeln, so konnten und können Unternehmen und andere Anwender doch davon ausgehen, dass die Papiere jedenfalls die vorherrschende Sichtweise der Aufsichtsbehörden der EU-Mitgliedstaaten zu den betreffenden Anwendungs- und Auslegungsfragen aufzeigen.

Viele Arbeitspapiere der Art.-29-Gruppe befassen sich mit den grundlegenden Fragen der EG-DSRL, etwa der Definition und Abgrenzung der Begriffe „Verantwortlicher" und „Auftragsdatenverarbeiter" (WP 169), dem auf Datenverarbeitungen anwendbaren nationalen Datenschutzrecht (WP 179), der Einwilligung (WPs 187, 194 und 208), dem Grundsatz der Zweckbindung (WP 203) oder Fragen der Anonymisierung (WP 216), um nur einige zu nennen. Andere Arbeitspapiere behandeln speziellere Themen wie etwa biometrische Daten (u.a. WP 193), Binding Corporate Rules (u.a. WP 153-155 und WP 195, 195a), Apps (WP 202), Cloud Computing (WP 196) u.v.m.. Insgesamt sind die Arbeitspapiere damit eine wahre Fundgrube an Auslegungs- und Anwendungshilfen für wichtige datenschutzrechtliche Fragen am Maßstab der EG-DSRL und anderer europäischer Datenschutzrechtsakte, etwa der e-privacy-Richtlinie.

Umso erstaunlicher ist, dass gerade in Deutschland der Bekanntheitsgrad der Arbeitspapiere der Art.-29-Gruppe bei vielen Unternehmen und anderen Akteuren lange Zeit offenbar nicht sonderlich hoch war. Auch in der Praxis der deutschen Datenschutzbehörden war bis vor nicht ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

allzu langer Zeit tendenziell nicht sehr häufig zu beobachten, dass auf Papiere der Art.-29-Gruppe und die darin entwickelten Aussagen und Maßstäbe verwiesen wurde. Deutlich häufiger als an den Arbeitspapieren der Art.-29-Gruppe orientierten sich die deutschen Aufsichtsbehörden an Beschlüssen und Positionen der deutschen Datenschutzkonferenz (DSK) oder des sog. Düsseldorfer Kreises (d.h. der Arbeitsgruppe der deutschen Aufsichtsbehörden für den nicht-öffentlichen Bereich). Dies lässt sich nur teilweise dadurch erklären, dass die Papiere der Art.-29-Gruppe nach der EG-DSRL lediglich Empfehlungscharakter haben; denn das gilt auch für Äußerungen der DSK oder des Düsseldorfer Kreises. Ein wichtigerer Grund dürfte in der föderalen Struktur der deutschen Datenschutzaufsicht liegen. Diese führte dazu, dass die Mehrzahl der deutschen Aufsichtsbehörden jeweils nicht selbst - d.h. durch eigene Mitarbeiter - an der Erarbeitung und Verabschiedung der einzelnen Arbeitspapiere auf europäischer Ebene, d.h. in der Art.-29-Gruppe und deren Facharbeitsgruppen (Subgroups), mitgewirkt hat. Vielmehr wirken die deutschen Aufsichtsbehörden in jeder Facharbeitsgruppe der Art.-29-Gruppe jeweils „nur“ durch einen Vertreter der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) sowie einen (maximal zwei) Vertreter der Aufsichtsbehörden der Bundesländer mit; in der Art.-29-Gruppe selbst, dem bisherigen „Spitzengremium“ der Aufsichtsbehörden auf EU-Ebene, wirken die deutschen Aufsichtsbehörden durch die BfDI sowie einen Repräsentanten der Aufsichtsbehörden der Länder (derzeit den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit) mit, die gemeinsam eine Stimme haben. An der Erstellung der Arbeitspapiere der Art.-29-Gruppe waren daher faktisch häufig jeweils nur einige wenige der deutschen Aufsichtsbehörden aktiv beteiligt. Konsequenz hiervon war oft, dass diese Papiere jedenfalls bis vor einiger Zeit nicht unbedingt immer im Fokus der Aufmerksamkeit und im Bewusstsein aller deutschen Aufsichtsbehörden präsent waren. In den letzten Jahren hat sich allerdings die Mitarbeit der deutschen Aufsichtsbehörden an der Erstellung von Arbeitspapieren der Art.-29-Gruppe stark intensiviert. Inzwischen haben die deutschen Aufsichtsbehörden ihre Informationsflüsse und Arbeitsprozesse so angepasst, dass sie nun alle eine effektive Möglichkeit zur Mitarbeit an der Entstehung der Arbeitspapiere der Art.-29-Gruppe und damit zur Einflussnahme auf die darin enthaltenen Positionen haben. In der Folge dieser Entwicklung sind der Bekanntheitsgrad und damit auch die praktische Relevanz der Arbeitspapiere der Art.-29-Gruppe auch in Deutschland zuletzt – bei Aufsichtsbehörden wie bei Unternehmen – doch merklich angestiegen.

Diese auch in Deutschland zuletzt verstärkte praktische Relevanz der Arbeitspapiere der Art.-29-Gruppe ist zu begrüßen. Denn spätestens durch die DS-GVO wird sich auch in Deutschland der Blick noch mehr als bisher auf Veröffentlichungen der Aufsichtsbehörden „auf europäischer Ebene“ konzentrieren müssen. Dies gilt sowohl für die Unternehmen und anderen Stellen, die die DS-GVO umsetzen müssen, als auch für die deutschen Aufsichtsbehörden. Letzteres schon deshalb, weil die DS-GVO für so genannte grenzüberschreitende Datenverarbeitungen vorsieht, dass sich alle von der Verarbeitung betroffenen und damit zuständigen Aufsichtsbehörden der Mitgliedstaaten miteinander abstimmen müssen. Lassen sich Meinungsverschiedenheiten unter den Behörden im konkreten Fall nicht ausräumen, ist eine verbindliche Entscheidung durch den EDSA im sog. Kohärenzverfahren herbeizuführen (Art. 65 DS-GVO). Vor diesem Hintergrund ist es für alle Datenschutzaufsichtsbehörden in der EU essentiell, so weit wie möglich ein einheitliches Verständnis der Vorschriften der DS-GVO zu entwickeln. Denn andernfalls muss die einzelne Aufsichtsbehörde in Fällen mit grenzüberschreitendem Charakter befürchten, mit der von ihr zu einer bestimmten Frage vertretenen Auffassung spätestens im Kohärenzverfahren im EDSA überstimmt zu werden. Damit erzeugt das Kohärenzverfahren der DS-GVO einen erheblichen faktischen Druck auf die Aufsichtsbehörden, auf ein gemeinsames Verständnis der Vorschriften der DS-GVO hinzuarbeiten.

Auch jenseits des Kohärenzverfahrens hat der EDSA gemäß Art. 70 Abs. 1 DS-GVO die Aufgabe, die einheitliche Anwendung der DS-GVO sicherzustellen. Zu diesem Zweck kann er gemäß Art. 70 Abs. 2 DS-GVO u.a. „Leitlinien, Empfehlungen und bewährte Verfahren“ bereitstellen, etwa zur Feststellung von Verletzungen des Schutzes personenbezogene Daten, zu Fragen der Datenlöschung, zur näheren Bestimmung der Kriterien und Bedingungen für Profiling, zur Festsetzung von Geldbußen, und darüber hinaus gemäß der „Generalklausel“ in Art. 70 Abs 1 lit. e DS-GVO auch zu allen weiteren Fragen, die für die einheitliche Anwendung der Verordnung relevant sind. Zwar haben Äußerungen, die der EDSA auf der Basis des Art. 70 DS-GVO trifft, keinen Gesetzescharakter. Jedoch kann man dabei durchaus von „soft law“ sprechen, da von den Leitlinien, Empfehlungen, bewährten Verfahren und weiteren Äußerungen des EDSA nach Art. 70 DS-GVO für die Praxis eine (deutlich) höhere Lenkungswirkung zu erwarten ist als von den bisherigen, auf die EG-DSRL bezogenen Arbeitspapieren der Artikel-29-Gruppe. Dies deshalb, weil die Rechtsanwender und die einzelnen Aufsichtsbehörden aus den weiter oben genannten Gründen davon ausgehen müssen, dass sich die Datenschutzbehörden der EU-Mitgliedstaaten, jedenfalls in ihrer Mehrheit, in noch stärkerem Maße an die Positionen des EDSA halten werden, als dies bei den Arbeitspapieren der Art.-29-Gruppe zum bisher geltenden Recht (insbesondere zur EG-DSRL) der Fall war. Dies schließt es freilich nicht aus, dass sich im Laufe der Zeit zu einzelnen Fragen, ggf. auch infolge von Gerichtsentscheidungen, durchaus auch einmal eine andere Position durchsetzen kann als die vom den EDSA zunächst vertretene.

Die DS-GVO bringt zwar gegenüber der EG-DSRL und den noch bis zum 24. Mai 2018 geltenden nationalen Gesetzen zu deren Umsetzung eine Reihe von Änderungen im Hinblick auf das materielle Datenschutzrecht, das von den Unternehmen und den anderen Verpflichteten einzuhalten ist. Nicht wenige Vorschriften der DS-GVO übernehmen jedoch nahezu unverändert oder doch in erheblichem Maße entsprechende Vorgänger-Regelungen der EG-DSRL. Beispielsweise entsprechen die Datenschutzgrundsätze des Art. 5 DS-GVO zumindest in weiten Teilen den bereits aus der EG-DS-RL bekannten Grundsätzen. Auch die Definitionen wichtiger Begriffe wie etwa „Verantwortlicher“, „Auftragsverarbeiter“ oder „Verarbeitung“ entsprechen, jedenfalls im Ergebnis, weitgehend der EG-DSRL. In solchen Fällen können daher Aussagen aus den existierenden Arbeitspapieren der Art.-29-Gruppe zunächst grundsätzlich auch für die Auslegung der entsprechenden „Nachfolgevorschriften“ aus der DS-GVO herangezogen werden.

Aus diesem Grunde kann es für Unternehmen und andere Rechtsanwender sehr lohnend sein, die existierenden Arbeitspapiere der Artikel-29-Gruppe zu konsultieren, die eine wahre Fundgrube an Interpretationshilfen zum bisherigen europäischen Datenschutzrecht, insbesondere zur EG-DSRL, bieten. Dabei ist freilich mit Blick auf die DS-GVO Sorgfalt geboten, da die Papiere an Stellen, an denen die DS-GVO Rechtsänderungen gegenüber der EG-DSRL bringt, natürlich nicht vollständig auf die Rechtslage nach der DS-GVO übertragbar sind.

Hinzuweisen ist in besonderem Maße noch darauf, dass die Erarbeitung künftiger Leitlinien des EDSA zur Auslegung der DS-GVO bereits seit dem Inkrafttreten der DS-GVO im Jahr 2016 in vollem Gange ist. Diese Arbeit findet laufend in der Art.-29-Gruppe statt, die inzwischen bereits mehrere „Guidelines“ (Leitlinien) zu zentralen Themen der DS-GVO veröffentlicht hat, darunter zum Datenschutzbeauftragten, zur Festlegung der federführenden Aufsichtsbehörde bei grenzüberschreitenden Datenverarbeitungen, zur Datenportabilität sowie zur Datenschutz-Folgenabschätzung (WP 242rev.01, 243rev.01, 244rev.01 und 248rev.01; veröffentlicht auf der letztgenannten der beiden o.g. Websites). Vorgesehen ist, dass der EDSA ab dem 25. Mai 2018 – also ab dem Zeitpunkt der Anwendbarkeit der Verordnung – diese und weitere bis dahin von der Art.-29-Gruppe bereits mit Blick auf die DS-GVO veröffentlichte und noch zu veröffentlichende Auslegungshilfen förmlich als „Leitlinien“

▸

im Sinne des Art. 70 DS-GVO beschließt. Unternehmen und anderen Anwendern kann daher geraten werden, gerade diese speziell auf die DS-GVO ausgerichteten neueren Veröffentlichungen der Artikel-29-Gruppe zu konsultieren, um sich auf die DS-GVO vorzubereiten.

Spätestens mit der Vorbereitung auf die DS-GVO sollten daher die Veröffentlichungen der Art.-29-Gruppe – und dies schließt durchaus, jedenfalls im Grundsatz, auch ältere Veröffentlichungen ein, die noch nicht speziell auf die DS-GVO gemünzt waren – auch in Deutschland in den Mittelpunkt der Aufmerksamkeit aller Unternehmen und sonstigen Stellen genommen werden, die dem EU-Datenschutzrecht unterliegen.

Über den Autor

Alexander Filip

Regierungsdirektor, Referatsleiter beim Bayerischen Landesamt für Datenschutzaufsicht

Anzeige

DATENSCHUTZ | SAP SECURITY | INFORMATIONSSICHERHEIT | IT-SECURITY

Datenschutz-Manager

Das Datenschutzmanagementsystem für den DSB – gemäß DS-GVO

EU ready

> Sofort einsetzbares System um den Überblick im Datenschutz zu behalten und Risiken effektiv zu erkennen und zu behandeln
> Inhaltlich ausgearbeitete Struktur, ausgerichtet an gesetzlichen Vorgaben und internationalen Normen 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

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

HERAUSFORDERUNG „EU-DATENSCHUTZ-GRUNDVERORDNUNG“ – DIE KUNST DER ERFOLGREICHEN UMSETZUNG

Detlef Klett, Mareike Gehrmann, Julian Klett

Nach einer Umfrage unter mehr als 200 IT- und Digitalunternehmen im Auftrag des Bitkom[1] gaben 19 Prozent der befragten Unternehmen an, sich bislang noch nicht mit der Umsetzung der EU-Datenschutz-Grundverordnung (DS-GVO) zu beschäftigen. Nur 34 Prozent der befragten Unternehmen gab an, erste Maßnahmen ergriffen oder bereits umgesetzt zu haben. Erst 42 Prozent der befragten Unternehmen beschäftigten sich nach der Umfrage überhaupt erst mit dem „Thema“, ohne jedoch zugleich Maßnahmen ergriffen zu haben.

Dieses Ergebnis ist mit Blick auf die drohenden Bußgelder, welche bei Verstößen in Höhe von bis zu EUR 20.000.000,00 oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres drohen und die laufende Umsetzungsfrist bis zum 25. Mai 2018 bemerkenswert. Der nachfolgende Beitrag soll deshalb mit Tipps aus der Praxis helfen, die „Scheu“ vor einem solchen Umsetzungsprojekt zu nehmen.

I. Warum fällt der Einstieg in ein DS-GVO Umsetzungsprojekt so schwer?

Die Umsetzung der DS-GVO stellt viele Unternehmen vor eine große Herausforderung. Dies liegt zum einen daran, dass die DS-GVO für datenschutzrechtliche Laien nur sehr schwer verständlich ist. Die Unternehmen wissen also oft nicht, wie sie einen sinnvollen Einstieg in ein Umsetzungsprojekt finden können. Zum anderen lässt sich durch die Umsetzung der Vorgaben der DS-GVO alleine kein Gewinn erzielen. Folglich fällt es den meisten Unternehmen ▸

[1] Quelle: https://www.bitkom.org/Presse/Presseinformation/Jedes-fuenfte-IT-Unternehmen-ignoriert-bislang-Datenschutzgrundverordnung.html

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

schwer, für ein Umsetzungsprojekt Personal oder Budget bereitzustellen.

Die Anforderungen der DS-GVO bedingen zudem, alle technischen und organisatorischen Datenverarbeitungsvorgänge auf den Prüfstand zu stellen. Da eine solche Überprüfung gelegentlich nicht nur positive Ergebnisse liefert, besteht bei einzelnen Verantwortlichen insoweit eine ablehnende Haltung. Auch besteht die Befürchtung, dass sich im Zuge der Umsetzung der DS-GVO Zuständigkeiten verschieben oder neu ergeben könnten.

Letztlich sind von der Umsetzung eine Vielzahl von Fachabteilungen in einem Unternehmen betroffen – vom Datenschutzbeauftragten über die IT, das Marketing und den Vertrieb bis hin zur Rechtsabteilung. Es sind demnach eine Reihe von Akteuren einzubinden. Alleine die Koordination aller Beteiligten stellt die Unternehmen schon vor eine große Herausforderung.

II. Wie das DS-GVO-Umsetzungsprojekt erfolgreich wird

1. Schritt 0: Projektinitiierung

Üblicherweise wird empfohlen, ein Umsetzungsprojekt mit der sogenannten „Gap-Analyse" zu starten. Dieser Ansatz berücksichtigt jedoch nicht die vorstehend genannten Herausforderungen an den Projekteinstieg. Noch vor Start des Umsetzungsprojekts sollten deshalb eine Reihe vorbereitender Maßnahmen vorgenommen werden.

Wie bei vielen Projekten sollte zuerst ein Projektleiter bestellt werden, welcher die Fähigkeit und die Befugnisse hat, das Projekt durchzusetzen. Dieser muss sich den Rückhalt der Geschäftsführung sichern. Nur mit ihrer Zustimmung und Förderung wird ein Umsetzungsprojekt nämlich gelingen.

Sodann muss eine realistische Kosten- und Ressourcenplanung vorgenommen und von der Geschäftsführung freigegeben werden. Hierbei ist insbesondere die Frage zu beantworten, ob externe Berater hinzugezogen werden sollen. Typischerweise erfolgt die externe Unterstützung durch Juristen. In Betracht zu ziehen ist aber auch die zusätzliche Hinzuziehung von technisch/organisatorischen Beratern. Dies hat den Vorteil, dass neben den Anforderungen an den Datenschutz zugleich die Anforderungen an die IT-Sicherheit umgesetzt werden können. Außerdem verfügen solche Berater regelmäßig über ein tiefes Wissen im Bereich Prozesse und Organisation.

Nun kann man sich den Vorbehalten der Mitarbeiter und Verantwortlichen annehmen. Hierzu könnte ein Workshop zum Thema „DS-GVO" stattfinden, in welchem die Anforderungen und Auswirkungen der DS-GVO sowie anschließend der Projektverlauf erläutert werden. Im Rahmen dieses Workshops könnten dann auch die Bedenken sowie etwaige Verbesserungsvorschläge der Beteiligten aufgenommen und von der Projektleitung berücksichtigt werden.

Letztlich wäre es wünschenswert, wenn die Geschäftsführung in einem angemessenen Maß dem Projekt Vorrang vor Tätigkeiten des operativen Geschäfts einräumen würde, um den Fachbereichen die Umsetzung der DS-GVO zu erleichtern.

2. Schritt 1: Gap Analyse

Nach dem mittlerweile üblichem Verfahren wird zunächst richtigerweise eine Gap-Analyse vorgenommen. Im Folgenden soll allerdings weniger die standardisierte Vorgehensweise beschrieben, als vielmehr praktische Tipps und Hilfestellungen zur erfolgreichen Durchführung dieser Phase gegeben werden.

Im Rahmen einer Gap-Analyse sollen die im Unternehmen bestehenden Datenschutz-Strukturen identifiziert und mit den Anforderungen der DS-GVO verglichen werden. Hieraus ergibt sich dann die zuschließende Lücke (Gap), welche den Handlungsbedarf aufdeckt. Die Gap-Analyse erfolgt also in zwei Phasen:

(1) Interviews

Nach der standardisierten Vorgehensweise erfolgen nun zunächst firmeninterne Interviews unter zur Hilfenahme von Fragebögen zur Identifizierung der bestehenden Datenschutz-Strukturen.

Neben der Tatsache, dass die Interviewbögen selbstverständlich alle Anforderungen der DS-GVO sowie die technischen und organisatorischen Gegebenheiten des betreffenden Unternehmens berücksichtigen müssen, sollte in der Praxis besonderes Augenmerk auf folgende Punkte gelegt werden:

i. Als Basis für die Erstellung der Interviewbögen sowie der Identifizierung der einzubindenden Fachbereiche ist es unerlässlich, als erstes zu erheben, welche Daten in welchen Systemen verarbeitet werden.

ii. Sodann muss anhand der vorstehend erwähnten Erhebung eine sorgfältige Auswahl der Gesprächspartner für die Interviews vorgenommen werden. Um ein möglichst vollständiges Bild zu erhalten, hat es sich bewährt, zwei bis drei Personen aus jedem Fachbereich vorzusehen.

iii. Für die Interviews sollte genügend Zeit, zirka drei Stunden pro Interview, eingeplant werden.

iv. Es ist zwingend darauf zu achten, dass der internen Projektleiter den Interviews beiwohnt, damit dieser einen vollständigen Überblick erhält.

v. Für einen reibungslosen Ablauf der Interviews und um die notwendigen Informationen im Interview erheben zu können, empfiehlt es sich, den Teilnehmern vorher den Fragebogen zukommen zulassen, damit diese sich auf das Interview vorbereiten können.

vi. Selbstverständlich ist auf eine vollständige und nachvollziehbare Dokumentation der Interviews zu achten.

vii. Letztlich sollten die ausgefüllten Fragebögen den Interviewpartnern noch einmal zur Überarbeitung und Freigabe bereitgestellt werden.

(2) Gap-Analyse Report

Im Rahmen des Gap-Analyse Reports erfolgt eine Auswertung der Interviews in Spiegelung zu den Anforderungen der DS-GVO, um etwaige Lücken festzustellen. In den von den Autoren durchgeführten Projekten hat sich folgender Aufbau des Reports bewährt:

1. Executive Summary

2. Grundsätzliches

a. Hintergrund

b. Auftrag

c. Beschreibung der Methode

d. Struktur des Reports

3. Rechtlicher Rahmen der DS-GVO

a. Kernziele der DS-GVO

b. Struktur der DS-GVO

c. Erläuterung der wichtigsten Inhalte der DS-GVO

4. Datenschutz-Analyse

Für den Kern des Gap-Analyse Reports – also der Datenschutz-Analyse – empfiehlt sich eine Darstellung in Tabellenform. Dabei werden gegenübergestellt die Anforderungen der DS-GVO und die Ergebnisse der Interviews. Aufgrund dieser Gegenüberstellung können dann die Lücken zwischen der DS-GVO und der firmeninternen Datenschutz-Struktur identifiziert werden. In einer letzten Spalte empfiehlt es sich, die identifizierten Lücken gemäß ihrer Kritikalität mit einem Ampelsystem zu versehen.

Dies könnte in Tabellenform so aussehen:

Anforderung DS-GVO	Ergebnis Interview	Ergebnis Lücke	Kritikalität anhand Ampelsystem

3. Schritt 2: Risikoanalyse

Besteht aufgrund der im Gap-Analyse Report identifizierten Lücken die Gefahr, dass eine Schließung aller Lücken voraussichtlich nicht bis zum 25. Mai 2018 erreicht werden kann, kann es sich empfehlen, eine Priorisierung vorzunehmen. Grundlage der Priorisierung ist eine Risikoanalyse. Diese kann anhand folgender Kriterien erfolgen:

- Kritikalität der jeweils zu verarbeitenden Daten,
- Art der Datenverarbeitung,
- Ort der Datenverarbeitung,
- Intensivität des Kundenkontakts und damit Höhe der Wahrscheinlichkeit der Geltendmachung der Betroffenenrechte,
- Gegebenenfalls in der Vergangenheit datenschutzrechtlich relevante Vorfälle des Unternehmens, welche von den Datenschutzbehörden verfolgt wurden,
- Höhe der bei einem Verstoß drohenden Bußgelder.

▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

4. Schritt 3: Umsetzung

Die Umsetzung sollte nun entsprechend der Priorisierung vorgenommen werden. Da die notwendigen Maßnahmen an den identifizierten Lücken ausgerichtet werden müssen, sind sie sehr unternehmens- und projektspezifisch, sodass allgemeine Aussagen grundsätzlich kaum möglich sind. Dies gilt insbesondere für die Implementierung erforderlicher neuer technischer und organisatorischer Maßnahmen. Schließlich ist hierbei zu berücksichtigen, dass viele Anforderungen der DS-GVO (z.B. die Betroffenenrechte und Meldepflichten) sowohl durch technisch-organisatorische als auch durch rein organisatorische oder rein technische Lösungsmöglichkeiten umgesetzt werden können.

Da vor allem die Einführung neuer technischer Maßnahmen sowie eine gegebenenfalls in diesem Zusammenhang erforderliche Neustrukturierung der IT- und Datenverarbeitungssysteme im Unternehmen oder sogar in der gesamten Unternehmensgruppe in der Regel viel Zeit und erhebliche personelle und finanzielle Ressourcen erfordern, kann es in Einzelfällen empfehlenswert sein, zunächst nur (organisatorische) Interimslösungen einzuführen. Hierdurch kann zum einen eine fristgerechte Einhaltung der Anforderungen bis zum 25. Mai 2018 und zum anderen eine vergabekonforme und (durchdachte) technische Gesamtlösung sichergestellt werden. Denn nicht selten sind bei einer Umstrukturierung der IT- und Datenverarbeitungssysteme auch weitere rechtliche und wirtschaftliche Aspekte zu berücksichtigen.

Die besondere Herausforderung in der Umsetzungsphase liegt aber vor allem darin, dass die Maßnahmen auf Ebene der Fachabteilungen stattfinden müssen. Der Projektleitung kommt hierbei insbesondere die Aufgabe zu, alle Beteiligten inklusive der externen Berater zu koordinieren sowie den Stand der Umsetzung nachzuverfolgen und gegebenenfalls korrigierend einzugreifen.

Hierbei muss das Unternehmen ein besonderes Augenmerk auf die Dokumentation legen. Die DS-GVO sieht nämlich umfangreiche Dokumentationspflichten, insbesondere bei etwaigen Ermessensentscheidungen bezüglich der Einführung neuer Maßnahmen, vor. Viele Entscheidungen sind deshalb im Rahmen einer gut zu dokumentierenden Abwägung zu treffen. Denn sollte in Zukunft der Verdacht eines Datenschutzverstoßes vorliegen, wird das Unternehmen nur auf Basis einer hinreichenden Dokumentation sein datenschutzkonformes Handeln beweisen können. Darüber hinaus wird der Dokumentation auch bei etwaigen Datenschutzverstößen im Hinblick auf die Bemessung des Bußgelds eine zentrale Bedeutung zukommen. Es ist deshalb für jedes Unternehmen unabdingbar, auch für die Zeit nach dem Umsetzungsprojekt einen Prozess zu etablieren, der eine umfassende Dokumentation sicherstellt. Dieser Prozess ist regelmäßig zu überprüfen und zu aktualisieren.

Neben der Einführung technischer und organisatorischer Maßnahmen wird auch die Anpassung der entsprechenden juristischen Dokumente erforderlich sein. Aufgrund der hohen Anzahl von Vereinbarungen, die konzernintern sowie mit Dritten geschlossen werden müssen, ist es essentiell, zunächst eine durchdachte Strategie für das Management von Datenverarbeitungsverträgen zu entwickeln. Die „Umformulierung" der einzelnen Dokumente ist dann nur der zweite Schritt.

Unbeschadet sämtlicher vorgenannter Maßnahmen wird es letztlich jedoch entscheidend sein, die eigenen Mitarbeiter umfassend und regelmäßig datenschutzrechtlich zu schulen. Denn um sicherzustellen, dass die implementierten Maßnahmen „greifen", bedarf eines grundlegenden datenschutzrechtlichen Verständnisses aller Mitarbeiter.

III. Fazit

Die Herausforderungen, mit denen sich die Unternehmen im Rahmen der Umsetzung der DS-GVO konfrontiert sehen, sind groß. Dennoch sollte sich schon aufgrund der Höhe drohender Bußgelder jedes Unternehmen diesen Herausforderungen stellen. Eine strukturierte und gut geplante Herangehensweise ist dabei Garant für ein erfolgreiches Umsetzungsprojekt.

Über die Autoren

Detlef Klett

Rechtsanwalt, FA für IT-Recht und Partner der internationalen Wirtschaftskanzlei Taylor Wessing am Standort Düsseldorf

Mareike Gehrmann

Rechtsanwältin, FAIn für IT-Recht und Salary Partnerin der internationalen Wirtschaftskanzlei Taylor Wessing am Standort Düsseldorf

Julian Klett

Wissenschaftlicher Mitarbeiter im Team von Detlef Klett am Standort Düsseldorf

Detlef Klett und Mareike Gehrmann sind spezialisiert auf die Technologie-Branche und den Bereich Datenschutz. Dort beraten sie Unternehmen und Behörden bei der Umsetzung komplexer Digitalisierungs- und Datenschutzprojekte sowie zu IT-sicherheitsrechtlichen Fragestellungen.

▶ www.taylorwessing.com

TaylorWessing

Anzeige

DQS CAMPUS – eine gute Entscheidung

THE AUDIT COMPANY

Datenschutz-Grundverordnung:
Was mein Unternehmen zur Umsetzung wissen muss.
Der Countdown zur Umsetzung der Datenschutz-Grundverordnung (DS-GVO) läuft: Der 25. Mai 2018 als Umsetzungsstichtag ist bereits in Sichtweite. Eine frühzeitige Kenntnis der neuen Anforderungen ist besonders wichtig, damit noch fehlende Prozesse eingeführt und etwaige Korrekturen an bestehenden Geschäftsprozessen vorgenommen werden können. In unseren Veranstaltungen vermittelt der Datenschutz-Experte und DQS-Auditor Stephan Rehfeld, wie die neuen Anforderungen optimal umgesetzt werden können.

Jährlich absolvieren 1.200 Teilnehmer Workshops mit uns!

Webinare

Prüfung der Rechtmäßigkeit und Datenverarbeitung nach Treu und Glauben
17. November 2017

Informationssicherheit bei der Verarbeitung personenbezogener Daten
8. Dezember 2017

Prozesse gestalten rund um die Rechte der Betroffenen
9. Februar 2018

Verträge zur Auftragsverarbeitung
16. Februar 2018

Workshop

Anfangen, planen, machen – Umsetzung der DS-GVO
Impulse von Profis, intensiver Austausch, vertiefende Arbeitseinheiten in kreativer Atmosphäre: Erfahren Sie mehr über die zeitlichen Vorgaben, die fundamentalen Datenschutzprinzipien und -mechanismen der DS-GVO. Gemeinsam identifizieren wir die erforderlichen Prozesse und erstellen einen Projektfahrplan zur praktischen Umsetzung der neuen gesetzlichen Anforderungen.
20. Dezember 2017 und 15. Januar 2018
in Frankfurt am Main

Unsere rund 60-minütigen Webinare und ganztägigen Workshops sind kostenpflichtig.
Weitere Veranstaltungen, ausführliche Informationen und Anmeldung unter **www.dqs-veranstaltungen.de**

DQS GmbH
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

Frankfurt am Main ▪ Berlin ▪ Hamburg ▪ München ▪ Stuttgart
info@dqs.de ▪ www.dqs.de

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

CHECKLISTEN ALS HILFSMITTEL ZUR UMSETZUNG DER DS-GVO[1]

Michael Punz

Datenschutz ist kein Zustand, sondern ein Prozess. Und dieser Prozess hat viele Verbindungen in die Welt der Informationssicherheit. Durch diese Komplexität ist es von großer Wichtigkeit, den Überblick bei der Umsetzung der Bestimmungen der DS-GVO in der eigenen Organisation zu behalten. Aus diesem Grund hat der „Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – Privacyofficers.at[2]" eine kompakte Checkliste zur Umsetzung der DS-GVO erstellt und publiziert. Im Weiteren erfolgt ein Einblick in den Aufbau, die Anwendung und die Entstehung dieser Checkliste.

Aufbau der Checkliste

Diese Checkliste wurde in drei Phasen gegliedert, um die wichtigsten Inhalte der DS-GVO übersichtlich abzubilden. Die erste Phase **„Vorbereitung"** beschreibt sinnvolle Maßnahmen, die im Vorfeld eines Umsetzungsprojektes durchgeführt werden sollten. In der zweiten Phase **„Umsetzung"** geht es um die inhaltliche Erarbeitung und Umsetzung der gesetzlichen Bestimmungen aus der DS-GVO. Abschließend fasst die dritte Phase **„Laufende Tätigkeiten"** all jene Tätigkeiten zusammen, die im laufenden Betrieb des DSMS[3] – nach Abschluss des Umsetzungsprojektes – beachtet werden sollten.

In jeder Phase sind mehrere Arbeitspakete enthalten. Alle Arbeitspakete beinhalten jeweils in kompakter Form eine Beschreibung des Arbeitspakets, eine Zielsetzung sowie eine Beschreibung der durchzuführenden Tätigkeiten. Weiterführende Informationen (z.B. aus Gesetzen, Normen usw.) können dann aus den ebenfalls in den Arbeitspaketen enthaltenen Referenzen, entnommen werden.

Zielgruppe

Die Checkliste wurde primär mit dem Fokus erstellt, einen managementtauglichen Überblick über die Anforderungen der DS-GVO zu geben. Somit zielt diese Checkliste u.a. auf Geschäftsführer, IT-Leiter, Informationssicherheitsbeauftragte, Datenschutzbeauftragte, Projekt-Manager und Entscheidungsträger, die sich mit der Umsetzung der DS-GVO-Bestimmungen befassen, ab.

Historie

Die erste Version der Checkliste wurde am 24. Mai 2017 (somit ein Jahr vor dem Geltungsbeginn der DS-GVO) unter einer Creative Commons 4.0-Lizenz veröffentlicht und wurde anschließend um die wichtigsten Bestimmungen aus dem österreichischen Datenschutz-Anpassungsgesetz 2018[4] sowie um diverse inhaltliche Änderungen und Referenzen ergänzt.

Die überarbeitete Version der Checkliste (derzeit in der Version 2.0) wurde am 9. September 2017 unter den gleichen Lizenzbedingungen publiziert und wird derzeit aufgrund der großen Nachfrage ins Englische übersetzt.

Anwendung der Checkliste in der Praxis

Bei der Strukturierung der Checkliste wurde darauf geachtet, dass die Anordnung der Phasen und Arbeitspakete in **chronologischer Reihenfolge** abgebildet wurde. Somit kann eine Organisation diese Checkliste auch als rudimentären Projektstrukturplan für die Umsetzung der DS-GVO verwenden. Allerdings sollte hierbei beachtet werden, dass einige Arbeitspakete längere Durchlaufzeiten haben (z.B. Verfahrensverzeichnis erstellen) und daher empfohlen wird, mehrere Arbeitspakete parallel zu bearbeiten. Jedes Arbeitspaket enthält auch einen Kurzstatus, ob sich das Arbeitspaket gerade „in Arbeit" befindet oder „erledigt" ist.

In ausgewählten Arbeitspaketen wurden auch Kontrollfragen integriert, um die jeweiligen gesetzlichen Anforderungen besser einordnen zu können. Dadurch soll auch ein besseres und praxistauglicheres Verständnis über die zentralen Inhalte der DS-GVO hervorgerufen werden.

Kontrollfragen

Beispiel: Datenschutz-Grundsätze

Im Arbeitspaket 2.4 „Einhaltung der Datenschutz-Grundsätze sicherstellen" sind nicht nur die Datenschutz-Grundsätze definiert, sondern es wurden auch jeweils Kontrollfragen hinterlegt, wie beispielsweise zum Datenschutz-Grundsatz „Datenminimierung":

> *„Werden tatsächlich alle diese personenbezogenen Daten benötigt oder kann der gleiche Zweck auch mit weniger bzw. ohne personenbezogene Daten erreicht werden?"*

Inhalt der Checkliste

Phase 1: Vorbereitung

In der ersten Phase geht es vorwiegend darum, entsprechende Sensibilisierungsmaßnahmen hinsichtlich der DS-GVO für das verantwortliche Management in der Organisation zu schaffen und die ersten Schritte für ein erfolgreiches Projekt vorzubereiten. Dabei sollen nicht die Konsequenzen bei Verstößen im Vordergrund stehen, sondern es sollen die Vorteile für eine Organisation betont werden, die sich durch eine angemessene Umsetzung der gesetzlichen Bestimmungen ergeben (z.B. positive mediale Berichterstattung, Unterscheidungsmerkmal zur Konkurrenz, neue Marktchancen usw.).

In einem weiteren Schritt wird der Projektauftrag finalisiert, in dem Ziele und Nicht-Ziele vereinbart, Projektphasen und Arbeitspakete definiert, Meilensteine erarbeitet und das Projektteam und Budget festgelegt werden.

Der Aufbau eines DSMS ist ein organisationsübergreifendes Projekt. Daher ist es notwendig, Schlüsselpersonal aus den Fachbereichen zu schulen, welches als Multiplikator (z.B. für die Erhebung von Informationen für das Verfahrensverzeichnis) oder zur selbständigen Übernahme von Arbeitspaketen eingesetzt werden kann.

Phase 2: Umsetzung

Die Umsetzungsphase nimmt den größten Zeit- und Ressourcenaufwand ein. In einem ersten Schritt werden alle Verarbeitungstätigkeiten identifiziert und zentrale Fragestellungen, wie z.B. die Frage nach dem Zweck der Datenverarbeitung und der Herkunft der Daten, beantwortet. Anschließend können die gesammelten Informationen strukturiert in ein Verfahrensverzeichnis zusammengeführt und in diesem dokumentiert werden. Das Verfahrensverzeichnis ist das zentrale Element eines DSMS und ist u.a. auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

Für bestimmte Verarbeitungstätigkeiten ist eine Datenschutz-Folgenabschätzung durchzuführen, wenn definierte Kriterien aus Art. 35 DS-GVO oder dem Working Paper 248[5] ▸

[1] Datenschutz-Grundverordnung (VO [EU] 2016/679)

[2] https://www.privacyofficers.at

[3] Datenschutz-Managementsystem: Aufstellung von Verfahren und Regeln innerhalb einer Organisation, welche dazu dienen, den Datenschutz dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern

[4] http://www.ris.bka.gv.at/Dokumente/BglAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.html

[5] http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

der Art. 29-Gruppe zutreffen. Auch die Einhaltung der Datenschutz-Grundsätze ist entsprechend sicherzustellen. Hierzu können die in der Checkliste enthaltenen Kontrollfragen herangezogen werden (siehe Infobox).

Auf Basis der Implementierungskosten, des Stands der Technik, der Umstände und der Zwecke der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen werden anschließend technische und organisatorische Maßnahmen festgelegt und dokumentiert. Hierzu dient als Basis die international anerkannte Norm ISO/IEC 27001:2013, aus der die wichtigsten Anforderungen in die Checkliste überführt wurden.

Eine zentrale Anforderung der DS-GVO ist der Schutz personenbezogener Daten der Betroffenen. Daher sind die Betroffenenrechte entsprechend in der eigenen Organisation praxistauglich abzubilden und zu dokumentieren. Hierzu zählen das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit sowie das Recht auf Widerspruch. Darüber hinausgehend ist ein Einwilligungsprozess zu implementieren und auch die Informationspflichten sind entsprechend zu adressieren.

Sofern externe Dienstleistungen bezogen werden, sind die Auftragsverarbeiter entsprechend auf Datenschutz zu verpflichten. Bereits bei der Auswahl und Beauftragung des Auftragsverarbeiters sind bestimmte Rahmenbedingungen sicherzustellen und schriftlich zu vereinbaren.

Neu hinzugekommen sind die beiden Anforderungen „Data Protection by Design“ (Datenschutz durch Technikgestaltung) und „Data Protection by Default“ (Datenschutz durch datenschutzfreundliche Voreinstellungen). Diese beiden neuen Grundsätze sind in der Organisation zu berücksichtigen und z.B. in den Beschaffungsprozess zu integrieren.

Trotz eines DSMS kann es zu Datenlecks kommen, denn eine 100%ige Sicherheit gibt es bekanntlich nicht. Gerade in solchen Situationen ist es von größter Wichtigkeit zu wissen, wie am besten vorzugehen ist. Dieser Ablaufplan ist im Data-Breach-Prozess zu dokumentieren, sodass dieser im Notfall ohne Verzögerung ausgeführt werden kann.

Last but not least werden in der Datenschutz-Policy verbindliche und zentrale Datenschutzvorgaben aus Organisationssicht erarbeitet, die vom verantwortlichen Management in Kraft zu setzen sind. Mitarbeiter sind auf die DS-GVO-Vorschriften und die erarbeiteten Bestimmungen zu sensibilisieren.

Phase 3: Laufender Betrieb

Ist das Umsetzungsprojekt erfolgreich abgeschlossen, muss sichergestellt werden, dass das DSMS nicht nur „am Leben“ erhalten wird, sondern auch kontinuierlich weiterentwickelt und verbessert wird.

So sollte u.a. das Verfahrensverzeichnis stets aktuell gehalten werden, indem neue Verarbeitungstätigkeiten nicht nur identifiziert, sondern auch ehestmöglich in das Verfahrensverzeichnis aufgenommen werden. Durch regelmäßige Überprüfungen und Audits können die Wirksamkeit und Effizienz des DSMS sichergestellt und punktuelle Verbesserungen aufgezeigt werden. Abschließend wird empfohlen, Kontakte mit Behörden und Betroffenen zu pflegen, um im Anlassfall entsprechende Kommunikationskanäle zur Verfügung zu haben.

Fazit

Um die DS-GVO umzusetzen und ein praxistaugliches, und vor allem dauerhaftes DSMS aufzubauen, ist die von Privacyofficers.at erstellte Checkliste ein geeignetes Hilfsmittel, welche einen übersichtlichen Maßnahmenplan in drei Phasen ermöglicht. Die Checkliste ist der rote Faden, der sich durch das Projekt zieht. Jeder im Projektteam bekommt sozusagen einen „Handwerkskoffer“, mit dem er selbständig arbeiten kann und die Übersicht über das Umsetzungsprojekt behält. Privacyofficers.at wünscht Ihnen gutes Gelingen bei der Umsetzung der Bestimmungen aus der DS-GVO und hofft, dass Sie diese Checkliste dabei bestmöglich unterstützt.

Download der Checkliste

Die kompakte Checkliste zur Umsetzung der DS-GVO kann unter folgendem Link heruntergeladen werden:

https://www.privacyofficers.at/Privacyofficers_Checkliste_Umsetzung_DSGVO_v2.0.pdf

Über den Autor

Michael Punz

IT-Sicherheitsbeauftragter (CISO) bei x-tention Informationstechnologie GmbH in Wels und Vorstandsmitglied im „Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter

▶ Privacyofficers.at

privacyofficers

Anzeige

Werden Sie jetzt DSGVO-konform! GDPR

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

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

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

2B Advice PrIME ®

VERZEICHNIS VON VERARBEITUNGS-TÄTIGKEITEN

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

TOM DOKUMENTIEREN

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

SCHULUNGEN

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

PRÜFUNGEN

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

KOSTENLOSER WEBCAST

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

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

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

KONZERNDATENSCHUTZ IN DER DS-GVO – PRAKTISCHE UMSETZUNG IN EINER UNTERNEHMENSGRUPPE

Timo Ahland

Wie gelingt es, für eine Unternehmensgruppe den passenden Plan zu entwerfen, damit die Geschäftsleitung dem Ziel des europäischen Gesetzgebers nachkommen und ab dem Stichtag 25.5.2018 ihre Verantwortung wahrnehmen kann, dass im Unternehmen und beim unternehmerischen Handeln die Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden, so wie sie in Artikel 5 Absatz 1 der EU Datenschutz-Grundverordnung (DS-GVO) festgelegt sind?

Im Kern weisen Artikel 5 und die umfangreichen Regelungen der DS-GVO, zu der sich auch noch nationale Umsetzungsgesetze, wie das deutsche „BGDSG neu“ hinzugesellen, den Weg. Aber so anders als das bisherige Recht sind insbesondere die Vorschriften der DS-GVO noch unbekannt und zudem teilweise sehr abstrakt. Trotz erster Leitfäden der Aufsichtsbehörden auf europäischer und nationaler Ebene ist noch vieles unklar, denn auch diese tasten sich an die DS-GVO heran und die Aufgabe, das Unternehmen auf das neue Recht und die geänderten Rahmenbedingungen vorzubereiten, lässt sich als „moving target“ beschreiben. Dies verlangt dem Praktiker bei der Projektplanung und -durchführung eine gute Portion Agilität ab. Die Komplexität des Vorhabens, sich auf die DS-GVO vorzubereiten, erhöht sich für eine Unternehmensgruppe um ein Vielfaches, noch dazu wenn diese europa- oder gar weltweit tätig ist. Ein Patentrezept zur erfolgversprechenden Vorgehensweise gibt es dabei nicht, es hängt von der individuellen Ausgangslage jedes Unternehmens ab.

Wie geht man unternehmensübergreifende Themen an?

Eine gute Kenntnis der Geschäftsaktivitäten und ein Überblick über die Konzernstruktur in allen relevanten Landesgesellschaften erscheinen als Ausgangslage unerlässlich, um den passenden Plan zu fassen. Insoweit unterscheidet sich ein Projekt zum Datenschutz und der DS-GVO-Vorbereitung nicht von vielen anderen Projekten.

Es erscheint sinnvoll, vor Ort zu beginnen und dann den Blick europa- und weltweit zu weiten:

Welche Strukturen und Aufgaben bestehen national, handelt es sich dabei um den Hauptsitz der Unternehmensgruppe, existieren Niederlassungen? Welche Aktivitäten (Vertrieb, Produktion, Forschung & Entwicklung), Verwaltung (HR, Finanzen, Einkauf, Recht, Compliance, Logistik usw.), gibt es bei wem und sind diese zentral- oder dezentral aufgestellt. Handelt es sich bei den Niederlassungen um selbständige oder unselbständige, gibt es Dienstleistungsgesellschaften (shared service center), die für die Unternehmensgruppe zB Rechnungs- oder Personalwesen betreuen oder sind bestimmte Aufgaben ausgegliedert bzw. „outgesourct“?

Die gleichen Fragen stellen sich hinsichtlich der Struktur der Unternehmensgruppe innerhalb und außerhalb der EU (Hauptsitz, Niederlassungen, Aktivitäten), insbesondere auch vor dem Hintergrund eines auch in der DS-GVO fehlenden Konzernprivilegs für konzerninterne Datennutzungen, -transfers oder -verarbeitungsvorgänge.

Eine wesentliche Rolle spielt die Grundausrichtung – strukturierter Konzern mit eigenständigen Landesgesellschaften, Holdingstruktur mit Divisionen, oder Matrixorganisation – national, regional, global. Was ist mit Partnerschaften, Joint Ventures und Konsortien? Hier empfiehlt sich eine Analyse mit den Gesellschaftsrechtlern, um die grundlegende Frage - wer ist Verantwortlicher, gemeinsamer Verantwortlicher, Auftragsverarbeiter – zu klären. Dies hilft sodann essentielle Folgefragen zu beantworten, u.a.:

Wo ist die federführende Aufsichtsbehörde für die Unternehmensgruppe in der EU angesiedelt?

Welche Gesellschaft muss zukünftig einen Datenschutzbeauftragten bestellen, gemäß Art. 37 DS-GVO oder eventuell existierender speziellerer nationaler Vorgaben wie § 38 „BDSG neu“ in Deutschland?

Wie identifiziert man die wesentlichen Themen und priorisiert sie richtig?

Einerseits weisen die Antworten zu Struktur, Rollen, Aufgaben usw. den Weg zur Identifizierung der wesentlichen Themen und zur Priorisierung. Daneben ergeben sich diese aus den betriebenen und geplanten Geschäftsmodell(en) und -aktivitäten. Orientierungshilfe bietet die Klärung folgender Fragen:

- Was für Daten werden von wem erhoben, gespeichert, verarbeitet (bzw. erworben, weitergegeben usw.)
- Welche Daten sind geschäftsnotwendig, welche relevant, welche verzichtbar / „nice to have“ - heute und morgen, Stichworte: Digitalisierung und Vernetzung
- National, EU, ex EU – ggf. bestehen national unterschiedliche Schwerpunkte aufgrund tlw. variierender Rahmenbedingungen in den EU-Mitgliedsstaaten, unterschiedliche Ausprägung der Geschäftsaktivitäten, Größe und Komplexität der Niederlassungen von Ort zu Ort, Land zu Land.

Eine wesentliche Rolle spielt auch der individuelle Datenschutz-Compliance-Reifegrad der Organisation(en) national, in der EU und darüber hinaus, feststellbar u.a. anhand folgender Aspekte:

- Sind eine Datenschutzorganisation, ein Datenschutzmanagementsystem und z.B. ein aussagekräftiges und aktuelles Verfahrensverzeichnis vorhanden?
- Existieren Richtlinien, Prozesse und werden diese gelebt?
- Wie hoch ist der Sensibilisierungsgrad von verantwortlicher Geschäftsleitung, Management und Belegschaft?
- Gibt es definierte Stakeholder, Koordinatoren, Ansprechpartner – national, EU, ex EU?
- Ist das Thema rechtliche Compliance und insbesondere der Datenschutz als eines der definierten Compliance-Themen etabliert oder neu?

Ein wesentlicher Indikator für die Priorisierung der Vorgaben und Themen dürfte, insbesondere aus Risikomanagement-Gesichtspunkten, der zukünftige (maximale) Sanktionsrahmen sein. Drohen für Verstöße eher maximal 4 % als 2 % des Vorjahresumsatzes. Hierzu bieten zahlreiche Praxisleitfäden und Literatur detaillierte Übersichten.

Daneben sind aber auch wegfallende Anforderungen zu beachten: in Deutschland zB die Vorgabe des bisherigen § 5 BDSG zur Verpflichtung auf das Datengeheimnis, die Pflicht zur behördlichen Meldung bzw. Genehmigungsvorbehalte für Datenverarbeitungsverfahren und internationale Datentransfers in einzelnen EU-Mitgliedsstaaten wie Frankreich, Österreich oder Spanien.

Nach persönlichem Benchmarking dürften in jedem Fall die folgenden zehn Themenbereiche relevant sein, wobei Priorisierung und Umfang von Unternehmen zu Unternehmen variieren werden:

▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

- Betroffenenrechte (Rechte auf Auskunft, Vergessenwerden, Löschung, Korrektur, Datenübertragung) und Informationspflichten
- Klärung der Rechtsgrundlagen der Datenverarbeitung, Einwilligungserklärungen und ggf. Anpassungen (analog und digital - websites, zu beachten hierbei die noch ausstehende EU E-Privacy-Verordnung)
- Prozess zur Meldung von Verarbeitungstätigkeiten, Datenschutzfolgenabschätzung und Verzeichnis der Verarbeitungstätigkeiten als Herzstück des dokumentierten und risikobasierten Datenschutz-Management-Systems
- Prozess zur internen Erfassung, Bearbeitung und Meldung von Datenschutzvorfällen
- Check und ggf. Anpassung der technischen und organisatorischen Maßnahmen (erweiterte Dimension: Risiko für Betroffene tritt zu den Risiken fürs Unternehmen hinzu)
- Check und ggf. Anpassung der Auftragsverarbeitungsvertragsmuster und Auftragsverarbeitungsverträge
- Aktualisierung der Datenschutzkonzernrichtlinie(n)
- sofern erforderlich: Absicherung der internationalen Datentransfers im Konzern und zu Dritten
- Benennung von Datenschutzbeauftragten im EU-Ausland, sofern erforderlich (und Meldung an Behörden per 25.05.2018)
- Sensibilisierung und Training der Beschäftigten

Wen bezieht man intern ein und wie?

Was unweigerlich zur Frage führt, wen man intern in das Projekt einbeziehen sollte und in welcher Rolle. Sofern vorhanden, kommt der vorhandenen Datenschutzorganisation des Unternehmens in den meisten Fällen die führende Rolle bei der Vorbereitung der Unternehmen auf die DS-GVO zu. Ob sie dabei die Projektleitung übernimmt, oder die fachliche Führung, kommt sicher auf die Stellung, Größe und Expertise im Einzelfall an.

Zur Datenschutzorganisation gesellen sich in einer Unternehmensgruppe sodann alle ihr im weitesten Sinne zuzurechnenden funktionalen Datenschutzkoordinatoren, definierten Ansprechpartner, lokalen Datenschutzbeauftragten, jeweils – soweit vorhanden oder nun ggf. zu installieren – national und international, abhängig von der konkreten Unternehmensstruktur.

Wesentliche Unterstützer sind sodann Compliance- und Rechtsabteilung, IT, IT Sicherheit, Einkauf, Revision, Qualitätssicherung sowie mögliche Schnittstellenverantwortliche in den Geschäftsbereichen wie z.B. funktionale Compliancemanager. Die Kommunikationsabteilung spielt eine wichtige Rolle bei der Erstellung des Kommunikationsplanes intern und extern.

Von wesentlicher Bedeutung ist selbstverständlich, die Aufmerksamkeit und Unterstützung durch die Unternehmensleitung sowie die Leitung von Standorten und Niederlassungen national und international zu gewinnen. Vom „tone from the top“ dürfte im Einzelfall stark die Bereitschaft der Geschäftsfunktionen abhängen, sich im Projekt aktiv zu engagieren und damit der Erfolg des Projektes insgesamt. Deshalb ist es wichtig, die Geschäftsleitung und das Management von Beginn an ins Boot zu holen und ihnen ihre Verantwortung gemäß Art. 5 Abs. 2 DS-GVO transparent zu machen.

Ob sie der Projektleitung ein Mandat zum Zugriff auf Personal aus ihrem Verantwortungsbereich gewähren oder direkt konkrete Projektmitglieder benennen, hängt vom Einzelfall ab. Wichtig ist, dass diese Personen einen Überblick über „ihre Funktion“ und eine gute Anbindung an die Leitung haben, um in die Funktion hineinwirken zu können und dass sie mit adäquatem Zeitbudget ausgestattet sind.

Und wie bringt man das Thema DS-GVO sodann an die Geschäftsfrau und den Geschäftsmann?

Natürlich hängt dies entscheidend vom einzelnen Unternehmen und dessen Kultur ab, wie es sich mit Neuerungen und Veränderungen auseinandersetzt und welche Bedeutung die Verarbeitung von Daten und damit der Datenschutz für das Geschäft haben. In einem stark „datengetriebenen“ Unternehmen mit globaler Matrixorganisation, in dem personenbezogene bzw. -beziehbare Daten nahezu in allen Geschäftsprozesse eine große bis unverzichtbare Rolle spielen, kann ein integrativer Ansatz Erfolg versprechend sein:

- Aufzeigen des Themas und seiner Bedeutung, der zu erwartenden Veränderungen, Neuerungen und Verschärfungen durch die DS-GVO durch die Datenschutzexperten.
- Adressieren der notwendigen Unterstützung durch die Geschäftsprozessverantwortlichen bei der Identifikation der konkreten Auswirkungen auf die bestehende Geschäftsprozesse und geplante Geschäftsaktivitäten, da diese „ihr“ Geschäft am besten kennen.
- Gemeinsame Planung der notwendigen Maßnahmen für die Anpassung der Geschäftsprozesse, mit dem Ziel geringstmöglicher bzw. keiner Geschäftsunterbrechung, um den Unternehmenserfolg als gemeinsames Hauptziel nicht zu gefährden.
- Vorzug für zentrale und unternehmensweit einheitliche Vorgehensweisen, Prozesse, Tools und Muster, um ein einheitliches Datenschutz-Management-System zu schaffen.
- Gemeinsame Entscheidung über Verantwortlichkeiten, d.h. darüber wer was bis wann macht.
- Dabei geltende Grundsätze für alle Maßnahmen: pragmatisch, lösungsorientiert, risikobasiert, praktikabel und agil (wg. des „moving targets“ DS-GVO)

Wichtig ist es, ein klares Commitment aller Projektbeteiligten im gemeinsamen Kick Off als Startpunkt zu erzielen und die gemeinsamen Ziele zu definieren.

Während der Projektarbeit empfehlen sich sodann regelmäßige formale und dokumentierte Reportings über den Fortschritt, aber auch kurze inoffizielle Pulschecks mit dem Topmanagement, ad hoc oder von Zeit zu Zeit, um gegenseitig Feedback zu geben und Realitätschecks durchzuführen: Was sind die aktuelle Prioritäten des Geschäfts, passt der Projektplan dazu, wie stark sind die Belastungen für die im Projekt Mitarbeitenden.

Benötigt man externe Unterstützung und wenn ja, wofür?

Auch die Frage, ob externe Unterstützung für die Vorbereitung des Unternehmens auf die DS-GVO benötigt wird, wird jeweils im Einzelfall in Abhängigkeit von Aspekten wie Reifegrad der Datenschutz-Compliance, Ausstattung und Kompetenzen der Datenschutzorganisation am Hauptsitz und in den Niederlassungen im In- und Ausland, verfügbare interne Kapazitäten und Ressourcen zu beantworten sein. Weitere indikatoren, ob und wenn ja wofür externe Unterstützung benötigt wird, dürften sein:

- Wird Projektmanagement- und/oder Datenschutz(rechts)expertise benötigt?
- Ist eine Gap-Analyse zur Standortbestimmung vorgesehen?
- Benötigt die Datenschutzorganisation Entlastung bei Projektaufwandsspitzen/ beim Tagesgeschäft oder sonstigen Aktivitäten, um sich auf die DS-GVO konzentrieren zu können?
- Soll die Verpflichtung Externer zur eigenen Qualitätssicherung dienen oder werden ggf. strategische Partner ggü. den internen Funktionen oder in den Niederlassungen benötigt, insbes. falls dort keine eigene Datenschutzrolle existiert?

Zudem bedarf es bei Einschaltung verschiedener Externer z.B. durch Zentrale und Auslandsniederlassungen einer engen Abstimmung der internen Verantwortlichen mit allen beteiligten externen Beratern über die Gesamtprojektziele, sodass es nur dort, wo es aufgrund nationaler Sonderregelungen geboten ist oder wo es für die Unternehmensgruppe gesamthaft betrachtet unkritisch ist, zu lokalen Abweichungen und Sonderwegen kommt.

Empfiehlt sich die Kontaktaufnahme mit der Aufsichtsbehörde und wie stellt man diese her?

Die Kontaktaufnahme mit den Aufsichtsbehörden ist eindeutig zu empfehlen. Einmal etabliert, kann dieser Kontakt fortan beidseitig für eine kontinuierliche Beratung genutzt werden. Grundlage hierfür ist nach bisherigem Recht § 38 BDSG, zukünftig Art. 31, 57 DS-GVO.

Im ersten Schritt gilt es, sich kennen zu lernen und das Geschäftsmodell des Unternehmens zu erklären. Hilfreich kann es sein, sich mit Unternehmen aus demselben Bundesland zu vernetzen, ▸

Stakeholder wie Kammern und Verbände einzubinden und gemeinsam den Kontakt zu suchen oder an Veranstaltungen der Behörde und ERFA-Kreis-Treffen teilzunehmen. Durch die Begegnung von Behördenvertretern und Schlüsselpersonen der Unternehmen wie Datenschutzbeauftragten, CISO und Geschäftsführung kann die Basis für den Dialog über bedeutsame Themen und Fragestellungen wie die Ausgestaltung praktikabler Lösungen für die Implementierung der DS-GVO-Vorgaben gelegt werden.

Gesamtfazit und Ausblick

Die DS-GVO stellt alle Unternehmen und insbesondere international tätige Unternehmensgruppen vor große Herausforderungen. Dabei handelt es sich um einen Marathon, der nicht bis zum Wirksamwerden am 25.05.2018 abgeschlossen sein wird. Es ist geboten jetzt zu identifizieren, was bis zu diesem Stichtag umgesetzt sein muss und was längerfristig zu implementieren ist. Dabei muss akzeptiert werden, dass es bis auf Weiteres gewisse Unsicherheiten bei der Vorbereitung auf den neuen Rechtsrahmen gibt und dies kann auch kommuniziert werden.

Aber: Darin liegt auch eine große Chance: Gibt es (noch) keine klaren Vorgaben und Standards, dann schafft dies auch Bewegungsspielraum in der Praxis, den es klug zu nutzen gilt. Dies gibt uns die Möglichkeit, selbst zu interpretieren und Neues zu entwickeln. International ausgerichteten Unternehmensgruppen ermöglicht die DS-GVO erstmals, eine gemeinsame europäische Datenschutzsicht zu entwickeln.

Und: Wir sind nicht allein. Tauschen wir uns mit anderen Rechtsanwendern und den Aufsichtsbehörden aus und gleichen wir ab, was die anderen machen.

Über den Autor

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

Boehringer Ingelheim

Anzeige

- Interne & externe Datenschutzbeauftragte -

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

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

Als Berater schützen Sie Unternehmen vor Haftungsansprüchen - wir schützen Sie.

- exclusives Wording für BvD-Mitglieder (auf Berufsbild DSB zugeschnitten)
- Tätigkeit ‚Auditor für Datenschutz' beitragsfrei eingeschlossen
- niedrige Einsteigerprämie sowie professionelle Beratung

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

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

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

AUFTRAGSVERARBEITERHAFTUNG NACH DER DS-GVO – WAS ÄNDERT SICH IN DER PRAXIS?

Thomas Kahl

Die Haftung für Datenschutzverstöße im Rahmen der Auftrags(daten)verarbeitung (AV) ist kein „neues" Thema der EU-Datenschutz-Grundverordnung (DS-GVO). Die Neuerungen der DS-GVO rücken das Thema jedoch in ein neues Licht. Schon jetzt führt die Neuordnung der Verantwortlichkeit des Auftragsverarbeiters unter der DS-GVO zu erheblichen Diskussionen und Verhandlungs(mehr)aufwand im Rahmen der Anpassungen bestehender und Verhandlung neuer AV-Verträge.

1. Auftragsverarbeiterhaftung – Ist da was neu?

Die Antwort lautet: **JA!**

Spielten - in der Regel eher moderat ausfallenden – Bußgelder oder die Haftung für Schadensersatzansprüche Betroffener in der Vergangenheit keine oder nur eine untergeordnete Rolle für Auftragsverarbeiter, rückt die Datenschutz-Haftung des Auftragsverarbeiters weiter in den Fokus der Beteiligten, was auf drei Gründe zurückzuführen ist:

Erstens ordnet Art. 82 DS-GVO die Verantwortlichkeiten zwischen Auftragnehmer und Auftraggeber im Rahmen der Auftragsverarbeitung gemäß Art. 28 DS-GVO grundlegend neu, wobei insbesondere der unklare Wortlaut enorme Unsicherheiten für betroffene Unternehmen erzeugt, die sich – je nach Interpretation der Regelungen – einer enorm weitreichenden Haftung ausgesetzt sehen.

Zweitens führt der erhöhte Sanktionsrahmen der DS-GVO mit Bußgeldern von bis zu 20 Millionen Euro oder 4 % des weltweiten Vorjahresumsatzes des Unternehmens zu deutlich gestiegenen Risiken für den Auftragsverarbeiter, wobei Bußgelder nunmehr direkt gegen den Auftragsverarbeiter verhängt werden können (vgl. Art. 58 (2) lit. i) DS-GVO).

Drittens führt die erhöhte „Awareness" bei Datenschutzaufsichtsbehörden und Unternehmen zu einem erhöhten Durchsetzungsrisiko.

▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

2. Haftung des Auftragsverarbeiters – Was gilt heute?

Nach aktueller Rechtslage lastet die Haftung für Datenschutzverstöße im Rahmen der Auftragsdatenverarbeitung weitestgehend auf den Schultern des Auftraggebers. So ordnet § 7 BDSG an, dass lediglich die verantwortliche Stelle gegenüber dem Betroffenen für die unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung personenbezogener Daten Schadensersatz zu leisten hat.

Das BDSG kennt jedoch keinen gesonderten Betroffenen-Anspruch gegen den Auftragsdatenverarbeiter im Fall von Datenschutzverstößen (vgl. § 11 Abs. 1 Satz 2 BDSG), wovon Fälle des sog. ADV-Exzesses selbstverständlich ausgenommen sind. Bußgelder werden regelmäßig gegen den Auftraggeber, nicht den Auftragnehmer verhängt (vgl. § 43 Abs. 1 lit. 2b) BDSG).

Hiervon unberührt blieb in der Vergangenheit zwar die Haftung des Auftragsverarbeiter gegenüber dem Betroffenen nach allgemeinen deliktischen Grundsätzen (§§ 823 ff. BGB in Verbindung mit §§ 30, 31 BGB), deren Bedeutung jedoch wegen fehlender Beweiserleichterungen (vgl. § 280 Abs. 1 S. 2 BGB) regelmäßig gering waren.

3. Haftung & Auftragsverarbeitung – Was ändert sich?

Art. 82 DS-GVO weitet zunächst den "Basisschutz" für Betroffene erheblich aus. Betroffenenansprüche können in Zukunft auch gegen den Auftragsverarbeiter geltend gemacht werden (vgl. Art. 82 Abs. 1 DS-GVO). Dabei folgt Art. 82 Abs. 1 DS-GVO dem Grundsatz der Verschuldenshaftung, sieht jedoch in Abs. 3 eine Verschuldensvermutung zu Gunsten des Betroffenen vor. Der Auftragsverarbeiter wird in seiner Haftung jedoch in gewissem Umfang privilegiert und haftet nur, sollte er entweder rechtmäßige Weisungen nicht befolgt oder gegen die ihn betreffenden Vorgaben der DS-GVO verstoßen haben (vgl. Art. 82 Abs. 2 S. 2 DS-GVO). Welche Verstöße hiervon genau erfasst werden, ist unklar. Im Wesentlichen dürfte es sich hierbei jedoch um die Pflichten aus dem Auftragsverarbeitungsvertrag bzw. Art. 28 DS-GVO sowie die weiteren „direkten" Verantwortlichkeiten z.B. aus Art. 32 DS-GVO (Sicherheit der Verarbeitung) handeln.

Ergänzt werden die Grundsätze um eine gesamtschuldnerische Haftung für Auftraggeber und Auftragnehmer, die die effektive Durchsetzung der Ansprüche des Betroffenen gewährleisten soll (vgl. EG 146). Unklar scheint, ob der Auftragsverarbeiter auch ohne einen tatsächlichen Verantwortungsbeitrag in die gesamtschuldnerische Haftung einbezogen werden kann. Eine entsprechende Interpretation überzeugt jedoch wenig. Dem dürften neben dem Wortlaut bereits Sinn und Zweck der Regelung entgegenstehen, da regelmäßig ein ausreichender Schutz u.a. über die Verschuldensvermutung (Abs. 3) erreicht werden dürfte und für eine derart weitreichende Haftung auch eines Nichtverantwortlichen kein Raum sein dürfte. Folgerichtig muss der Auftragsverarbeiter zumindest für „irgendeinen", wenn auch untergeordneten Teil der geltend gemachten Schäden nach Art. 82 Abs. 2 und 3 DS-GVO verantwortlich sein, um in die Gesamtschuldnerschaft gem. Abs. 4 einbezogen werden zu können. Kann er sich exkulpieren, bleibt ihm dies erspart. Kann er es nicht, muss er ggf. in die volle Haftung gegenüber dem Betroffenen gehen, wenn dieser das fordert und sich auf den sog. Innenregress verlassen.

Abs. 5 regelt, wie dieser Innenausgleich zwischen Auftraggeber und Auftragnehmer (oder zwischen anderen Beteiligten wie z.B. zwei Verantwortlichen) zu erfolgen hat, wobei sich die Quotelung am Verantwortungsbeitrag zu orientieren hat. (Wohl) Deutlich einschneidender wird sich jedoch die bereits angesprochene Direktverantwortlichkeit für Bußgelder auswirken (vgl. Art. 58 (2) lit. i) DS-GVO), die Auftragsverarbeiter zukünftig ggf. deutlich öfter in die Schusslinie der Behörden bringen könnte, als dies bislang regelmäßig der Fall war.

4. Beschränkung der Auftragsverarbeiterhaftung – Was geht (noch) unter der DS-GVO?

Im Hinblick auf das unter der DS-GVO deutlich erweiterte Pflichten- und Haftungsprogramm des Auftragsverarbeiters stellt sich die Frage, welche Grenzen die Beteiligten bei der Ausgestaltung der Haftung im Innenverhältnis zu beachten haben und ob Haftungsbeschränkungen zu Gunsten des Auftragsverarbeiters nicht ggf. sogar generell im Widerspruch zu tragenden Grundprinzipien der DS-GVO stehen und deshalb ausgeschlossen sein müssen.

4.1 Was spricht dagegen?

Gegen die Möglichkeit von Haftungserleichterungen zu Gunsten des Auftragsverarbeiters ließen sich folgende Erwägungen ins Feld führen:

Haftungserleichterungen könnten das „neue" Haftungskonstrukt der DS-GVO aufweichen und verwässern. Es ließe sich argumentieren, dass so die Befolgung der strengen Vorgaben der DS-GVO mangels effektiver vertraglicher Sanktionsmöglichkeiten nicht mehr gewährleistet wäre und eine wesentliche Zielsetzung der Verordnung - die Schaffung eines hohen Datenschutzniveaus (vgl. EG 10) - vereitelt würde.

4.2 Haftungsbeschränkungen bleiben möglich

Ein genereller Ausschluss von Haftungsbeschränkungen im Innenverhältnis scheint jedoch nicht sachgerecht und wird in Grenzen des geltenden Rechts (dazu sogleich) weiterhin möglich bleiben.

Erstens enthalten weder Artikel 82 noch Artikel 28 DS-GVO ausdrückliche Verbote oder Anhaltspunkte, die auf entsprechende Restriktionen hindeuten.

Zweitens bestehen neben der vertraglichen Haftung des Auftragsverarbeiters weitere empfindliche (Sanktions-)Mechanismen, um diesen zur Einhaltung der DS-GVO zu motivieren, insbesondere durch Ordnungsmaßnahmen und Bußgelder. Abweichende Abreden zur Haftung im Innenverhältnis haben hierauf keinen Einfluss.

Drittens werden Betroffene durch Regelungen zum Innenverhältnis regelmäßig nicht benachteiligt, so dass die Durchsetzbarkeit der Betroffenenansprüche hierdurch nicht erschwert werden dürfte.

5. Haftungsregelungen nur unter Beachtung allgemeiner Grundsätze

Die Frage der Möglichkeit von Haftungserleichterungen bestimmt sich damit vielmehr nach den anerkannten Grundsätzen des nationalen (Zivil-) Rechts.

Die wesentlichen Grenzen zieht dabei das deutsche AGB-Recht in den §§ 305 ff. BGB, an denen sich formularmäßig vereinbarte Klauseln zur Haftung messen lassen müssen. Ausschlüsse in Formularverträgen für einfach fahrlässige Verletzung von Kardinalpflichten sowie grob-fahrlässige Pflichtverletzungen werden regelmäßig an § 309 Nr. 7 lit. b) BGB scheitern, der auch im Unternehmerverkehr Indizwirkung entfaltet. Summenmäßige Beschränkungen der Haftung in Formularverträgen sind bereits heute schwer bis kaum wirksam umzusetzen. Sollten Auftragsverarbeiter eine Beweislastumkehr in Formularverträgen zu ihren Gunsten vereinbaren wollen, könnte dies u.a. wegen § 280 Abs. 1 S. 2 BGB (Verschuldensvermutung) an § 309 Nr. 12 BGB bzw. § 307 BGB scheitern. Im Übrigen bleiben das Verbot überraschender Klauseln sowie das Transparenzgebot zu beachten (§ 305c BGB), die insbesondere bei über verschiedene Vertragsbestandteile „verteilte" Haftungsregelungen eine gewisse Sorgfalt erfordern, um keine intransparenten und folglich nicht mehr durchsetzbaren Regelungskonstrukte zu schaffen. Auf Grund der beschriebenen Beschränkungen durch die §§ 305 ff. BGB werden Auftragsverarbeiter auch zukünftig auf individuelle Haftungsbeschränkungen setzen.

Individualvertraglich setzen die §§ 134, 138 und 242 BGB die maßgeblichen Grenzen. Mit Ausnahme eines Haftungsausschlusses für vorsätzliche Datenschutzverstöße dürften Haftungsbeschränkungen zu Gunsten des Auftragsverarbeiters nach den bislang anerkannten Grundsätzen individualvertraglich vereinbart werden können, wobei insbesondere die Frage der Haftung des Auftragnehmers für gegen den Auftraggeber verhängte Bußgelder auf Grund der insoweit unklaren Regelungen der DS-GVO zu Diskussionen führen wird. ▸

6. Folgen für die Vertragspraxis

Die erweiterte Haftung des Auftragnehmers sowie die (weiterhin) bestehende Möglichkeit, diese sachgerecht im Auftragsverarbeitungsvertrag zu beschränken, führt schon jetzt zu einem erhöhten Verhandlungsbedarf bei der Umstellung von Alt-Verträgen und dem Neuabschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 DS-GVO.

Folgende Punkte werden Auftragsverarbeiter zu beachten haben, um die „neuen" Haftungsrisiken sinnvoll in den Griff zu bekommen:

Da Auftragsverarbeiter bei Nichtbeachtung rechtmäßig erteilter Weisungen nach Art. 82 Abs. 2 DS-GVO verantwortlich sind, werden klare Regelungen im Umgang mit Weisungen des Auftraggebers erforderlich, z.B. zu ggf. vorzunehmenden Prüfungen des Auftragsverarbeiters inklusive einer etwaigen Remonstrationspflicht, der ausreichenden Dokumentation und zum Umgang mit Weisungen, bei denen die Rechtsmäßigkeit unklar oder umstritten ist.

Auftragsverarbeiter werden versuchen, Beweiserleichterungen zu ihren Gunsten zu verhandeln, wobei die beschriebenen Grenzen des AGB-Rechts zu beachten sein werden. Vertraglich sollte insoweit geregelt werden, welche Nachweis-Mittel zur Dokumentation der Compliance und des erforderlichen Sorgfaltsmaßstabs genutzt werden können und welche Prüf-Standards für den konkreten Fall am geeignetsten erscheinen (z.B. Vorlage von spezifischen Testaten, spezielle Cloud-Zertifizierungen, besondere Prüfintervalle).

U.A. wegen Art. 82 Abs. 4 DS-GVO werden Auftragsverarbeiter vermehrt Modifikationen der Haftungsverteilung im Innenverhältnis und Freistellungen einfordern, wobei zumindest in Formularverträgen Vorsicht geboten ist, da insbesondere letztere Klauseln z.B. als überraschend eingestuft werden könnten (vgl. § 305 c BGB).

In jedem Fall sollten präzise Regelungen zum Umgang und zur Abwicklung von Drittansprüchen aufgenommen werden, z.B. welcher Beteiligte bei der Verteidigung in den „Lead" gehen soll, wer welche Kosten übernimmt und wie der Abstimmungsprozess im Detail erfolgt.

Summenmäßige Haftungsbeschränkungen speziell für Datenschutzverstöße werden weiterhin häufig gefordert und verhandelt werden, wobei hierfür meist individuelle Verhandlungen erforderlich sein werden, um den Beschränkungen des AGB-Rechts zu entkommen.

Im Übrigen werden insbesondere Auftragnehmer, die eigene Vertragsmuster verwenden, auf eine klare Struktur der Haftungsregelungen achten müssen, wenn diese zwischen Hauptvertrag und A(D)V-Vertrag verteilt sind, um nicht Gefahr zu laufen, dass einzelne oder im Ernstfall sogar alle Haftungsregelungen wegen Intransparenz undurchsetzbar werden.

7. Fazit

Auftragsverarbeiter werden unter der DS-GVO einmal mehr besonders gefordert. Die gute Nachricht: Trotz der verschärften Haftungsanforderungen wird sich im Rahmen der Auftragsverarbeitung auch zukünftig ein sinnvoller Ausgleich im Hinblick auf die Verantwortlichkeiten der Beteiligten finden lassen, wenn und soweit die beschriebenen „Spielregeln" beachtet werden und die Beteiligten es schaffen, sich auch auf interessengerechte Lösungen zu verständigen.

Der vorliegende Beitrag geht auf einen Vortrag des Verfassers bei der Herbstakademie der Deutschen Stiftung für Recht und Informatik (DSRI) 2017 zurück, der als schriftlicher Beitrag im Tagungsband Jürgen Taeger (Hrsg.), Recht 4.0 – Innovationen aus den rechtswissenschaftlichen Laboren, Edewecht 2017, veröffentlicht wurde.

Über die Autoren

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

▶ www.taylorwessing.com

TaylorWessing

Anzeige

Aktuell zur Datenschutz-Grundverordnung.

Jetzt handeln und Haftungsrisiken vermeiden.

Erleichtert den Aufbau der Datenschutzorganisation

Koreng/Lachenmann
Formularhandbuch Datenschutzrecht
2. Auflage. 2018. Rund 1000 Seiten.
In Leinen mit Online-Zugang ca. € 129,–
ISBN 978-3-406-69542-1
Neu im November 2017
Mehr Informationen:
www.beck-shop.de/bjzdaj

Ein Handbuch für die betriebliche Praxis

Forgó/Helfrich/Schneider
Betrieblicher Datenschutz
2. Auflage. 2017. LX, 1331 Seiten.
In Leinen € 209,–
ISBN 978-3-406-69541-4
Mehr Informationen:
www.beck-shop.de/bjzdai

Der »Wächter« für Ihre Daten

Wächter
Datenschutz im Unternehmen
5. Auflage. 2018. Rund 680 Seiten.
Kartoniert ca. € 65,–
ISBN 978-3-406-71525-9
Neu im November 2017
Mehr Informationen:
www.beck-shop.de/btnxgt

Der Kommentar für die Praxis

Gola
DS-GVO · Datenschutz-Grundverordnung VO (EU)
2017. XXII, 835 Seiten.
In Leinen € 79,–
ISBN 978-3-406-69543-8
Mehr Informationen:
www.beck-shop.de/bjzdap

Beck'scher Kompaktkommentar

Paal/Pauly
Datenschutz-Grundverordnung (DS-GVO)
2017. XXV, 891 Seiten. Gebunden € 99,–
ISBN 978-3-406-69570-4
Mehr Informationen:
www.beck-shop.de/bjzfas

Umfassende Kommentierung

Kühling/Buchner
DS-GVO · Datenschutz-Grundverordnung
2017. XVI, 1169 Seiten.
In Leinen € 159,–
ISBN 978-3-406-70212-9
Mehr Informationen:
www.beck-shop.de/blgsgd

Europäischer Blick aus erster Hand

Ehmann/Selmayr
Datenschutz-Grundverordnung
2017. XXXVI, 1243 Seiten.
In Leinen € 139,–
ISBN 978-3-406-70215-0
(In Gemeinschaft mit LexisNexis SA)
Mehr Informationen:
www.beck-shop.de/blgsgg

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

C.H.BECK

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

BESCHÄFTIGTENDATENSCHUTZ NACH DEM NEUEN BDSG

Tim Wybitul und Kai Wendt

Am 27. April 2017 hat der Bundestag das neue Bundesdatenschutzgesetz (BDSG-neu) verabschiedet. Zusammen mit der EU-Datenschutz-Grundverordnung (DS-GVO) soll es ab dem 25. Mai 2018 anwendbar sein. Mit dem BDSG-neu sollen unter anderem die zahlreichen Öffnungsklauseln der DS-GVO ausgefüllt werden.

I. Wie steht das BDSG-neu zur DS-GVO?

Die DS-GVO ist als EU-Verordnung gemäß Art. 288 Abs. 2 AEUV unmittelbar anwendbar. Sie wirkt daher direkt und ist ohne weitere nationale Umsetzungsgesetze verbindlich. Somit werden bisherige nationale Regelwerke im Bereich des Datenschutzes durch die DS-GVO verdrängt. In ausgewählten Angelegenheiten erlaubt die DS-GVO den Mitgliedstaaten jedoch ausdrücklich die Konkretisierung von Vorschriften durch nationale Rechtsvorschriften. Dazu gehört auch der für Unternehmen in der Praxis sehr relevante Themenbereich des Beschäftigtendatenschutzes.

1. Welche Vorgaben macht die DS-GVO zum Beschäftigtendatenschutz?

Art. 88 DS-GVO ermöglicht es dem nationalen Gesetzgeber, Datenschutzfragen im Beschäftigungsbereich in eigener Verantwortung zu konkretisieren. Zu den Anwendungsbereichen des Beschäftigtendatenschutzes zählt die DS-GVO u.a. die Einstellung, Erfüllung des Arbeitsvertrages und die Beendigung von Arbeitsverhältnissen. Eine wesentliche Abweichung von den grundsätzlichen Vorgaben der DS-GVO ist nicht zulässig. Art. 88 Abs. 1 DS-GVO enthält vielmehr die Vorgabe, dass auch nationale Regelungen den Schutz der Rechte und Freiheiten von Mitarbeitern im Zusammenhang mit Datenverarbeitungsvorgängen gewährleisten sollen. Die Umsetzung in das nationale Recht soll die allgemeinen Vorschriften der DS-GVO lediglich spezifizieren. Nach Art. 88 Abs. 2 DS-GVO umfassen die Vorschriften zudem angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte. Insbesondere sollen die Mitgliedstaaten bei den Vorschriften ein Augenmerk auf die Transparenz der Verarbeitung, auf die Übermittlung von Daten in Unternehmensgruppen bzw. in einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausführen, sowie auf Überwachungssysteme am Arbeitsplatz legen.

Die Umsetzung von Öffnungsklauseln in nationales Recht soll in der Regel in Form von Rechtsvorschriften erfolgen. Art. 88 Abs. 1 DS-GVO nennt allerdings auch ausdrücklich Kollektivvereinbarungen als Alternative zu Rechtsvorschriften für die Rechtmäßigkeit der Verarbeitung. Daher können etwa auch Betriebsvereinbarungen weiterhin die Verarbeitung personenbezogener Daten regeln bzw. erlauben.

2. Umsetzung des Beschäftigtendatenschutzes im BDSG-neu

Das BDSG-neu konkretisiert die Vorgaben zum Beschäftigtendatenschutz in § 26 BDSG-neu. Im Wesentlichen gleicht § 26 Abs. 1 BDSG-neu dem vorherigen § 32 Abs. 1 BDSG, erweitert diesen aber um Regelungen zur Verarbeitung personenbezogener Daten für betriebsverfassungsrechtliche Zwecke.

§ 26 Abs. 1 Satz 1 BDSG-neu erlaubt die Datenverarbeitung, soweit diese zu Zwecken der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses sowie zum Zweck der Erfüllung gesetzlicher, tarifvertraglicher und auf Kollektivvereinbarung basierender Pflichten erforderlich ist. § 26 Abs. 1 Satz 2 BDSG-neu regelt die Datenverarbeitung zur Aufklärung von Straftaten. Hinzugekommen sind insbesondere die Regelungen zur Einwilligung im Beschäftigungsverhältnis (§ 26 Abs. 2 BDSG-neu), zur Verarbeitung von besonderen Kategorien personenbezogener Daten (§ 26 Abs. 3 BDSG-neu) und Regelungen zur Datenverarbeitung auf Grundlage von Kollektivvereinbarungen (§ 26 Abs. 4 BDSG-neu). § 26 Abs. 7 BDSG-neu regelt zudem, dass sich die Vorschriften des Beschäftigtendatenschutzes nicht nur auf die automatisierte Verarbeitung erstrecken, sondern auf alle Verarbeitungsvorgänge, somit auch auf die nicht-automatisierten.

II. Inhaltliche Vorgaben von § 26 BDSG-neu

Zwar gleicht § 26 BDSG-neu dem bisher geltenden § 32 BDSG, dennoch wurden einige Neuerungen und Konkretisierungen mit eingebracht. Mit Blick auf die kommende Rechtsprechung, lässt die Regelung jedoch noch einige Fragen offen und viel Raum zur Interpretation und Auslegung. Der folgende Abschnitt stellt einige der Kernänderungen der Vorschrift und die Auswirkungen für die Praxis dar.

1. Datenverarbeitung muss für Zwecke des Beschäftigungsverhältnisses erforderlich sein

Nach § 26 Abs. 1 Satz 1 BDSG-neu dürfen Daten von Beschäftigten verarbeitet werden, wenn dies für die Zwecke des Beschäftigtenverhältnisses erforderlich ist. Das BDSG-neu enthält allerdings keine Definition für die Erforderlichkeit. Die Gesetzesbegründung gibt jedoch klare Hinweise darauf, wie Arbeitgeber den Begriff der Erforderlichkeit im Rahmen von § 26 BDSG-neu auslegen müssen. Der Gesetzgeber orientiert sich an der Rechtsprechung des EuGH und des BAG. Im Rahmen der Prüfung sind daher die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz gegeneinander abzuwägen (vgl. BT Drs. 18/11325, S. 97). Der Arbeitgeber muss einen Mittelweg finden, der beiden Positionen gerecht wird, ohne eine Seite zu sehr einzuschränken. Entsprechend muss die Verarbeitung für die vom Arbeitgeber verfolgten Zwecke geeignet, das mildeste von mehreren gleichermaßen effektiven Mitteln und angemessen sein. Eine Datenverarbeitung ist angemessen, solange die Interessen der Mitarbeiter nicht deutlich überwiegen, also nicht weit außerhalb von vernünftigerweise zu erwartenden Verarbeitungen liegen.

▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

2. Welche Vorgaben gelten bei der Aufklärung von Straftaten?

Gemäß § 26 Abs. 1 Satz 2 BDSG-neu dürfen wie bisher Daten von Mitarbeitern auch zur Aufdeckung von Straftaten verarbeitet werden. Dazu müssen dokumentierte und tatsächliche Anhaltspunkte den Verdacht begründen, dass der Mitarbeiter eine Straftat begangen hat. Die Verarbeitung muss erforderlich und verhältnismäßig sein. Außerdem darf das schutzwürdige Interesse des Beschäftigten nicht überwiegen. Beobachtet der Arbeitgeber im Rahmen einer gerechtfertigten Überwachung eines konkreten Arbeitnehmers, dritte Arbeitnehmer bei der Begehung von Straftaten, kann er diese Daten ebenfalls verarbeiten.

Das BDSG-neu enthält, wie schon unter der aktuellen Rechtslage nach dem BDSG, keine konkrete Regelung zu Datenverarbeitungen bei Anhaltspunkten für eine schwerwiegende Pflichtverletzung. Das BAG nimmt in seiner Rechtsprechung an, dass diese Verarbeitungen zur ordnungsgemäßen Durchführung des Arbeitsverhältnisses gemäß § 32 Abs. 1 Satz 2 BDSG erforderlich sind, da der Arbeitgeber hier seine Rechte zur Leistungs- und Verhaltenskontrolle wahrnimmt. Das BAG hat hierzu mittlerweile Klarheit geschaffen und eine gegenteilige Entscheidung des LAG Baden-Württemberg (Az. 4 Sa 61/15) aufgehoben (vgl. BAG Urt. v. 29.06.2017 – 2 AZR 597/16). Eine Klarstellung durch den Gesetzgeber wäre zwar zu begrüßen gewesen, ist aber für die Praxis entbehrlich. Das LAG Baden-Württemberg hatte in der Vorinstanz noch vertreten, dass Kontrollen zur Aufdeckung von Pflichtverletzungen unterhalb der Schwelle von Straftaten durch § 32 Abs. 1 Satz 2 BDSG gesperrt und dementsprechende Maßnahmen damit rechtswidrig seien. Das BAG stellt dagegen zu Recht fest, dass pauschale Verarbeitungsverbote weder mit der Gesetzessystematik noch mit Unionsrecht vereinbar sind. Vielmehr müsste in jedem Fall eine Verhältnismäßigkeitsprüfung vorgenommen werden, wobei auch bei der Aufklärung von schwerwiegenden Pflichtverletzungen ähnlich strenge Voraussetzungen zu stellen sind wie bei dem Verdacht einer Straftat.

3. Datenverarbeitung auf der Grundlage von Einwilligungen von Beschäftigten

§ 26 Abs. 2 BDSG-neu bestimmt die Voraussetzungen einer wirksamen Einwilligung im Beschäftigungsverhältnis. Demnach ist eine wirksame Einwilligung in Datenverarbeitungen nur möglich, wenn die Freiwilligkeit der Einwilligung besonders berücksichtigt wurde. Der Arbeitnehmer hat gerade in einem Arbeitsverhältnis eine gewisse Abhängigkeit vom Arbeitgeber. Diese Abhängigkeit könnte die Freiwilligkeit der Einwilligung beeinträchtigen. § 26 Abs. 2 BDSG-neu stellt beispielhaft dar, wann auch im Arbeitsverhältnis eine freiwillige und damit wirksame Einwilligung vorliegen kann. Hat der Arbeitnehmer durch die Einwilligung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder verfolgen beide Parteien gleichgelagerte Interessen, kann demnach eine freiwillige Einwilligung vorliegen. Die Einwilligung bedarf grundsätzlich der Schriftform, außer wenn wegen besonderer Umstände eine andere Form angemessen ist (z.B. in elektronischer Form). Der Arbeitnehmer ist ferner in Textform über den Zweck der Verarbeitung sowie über sein Widerrufsrecht aufzuklären.

Die Artikel-29-Datenschutzgruppe (Art.-29-Gruppe) hat erst im Juni 2017 in ihren Leitlinien zum Beschäftigtendatenschutz (WP 249) eine Einwilligung im Beschäftigungsverhältnis als sehr kritisch beurteilt. Darüber hinaus rät die Art.-29-Gruppe Arbeitgebern sogar grundsätzlich von einer Einwilligungslösung ab. Das BAG geht allerdings davon aus, dass auch in einem Arbeitsverhältnis der Betroffene frei entscheiden könne und eine Einwilligung grundsätzlich möglich sei (BAG Urt. v. 11. Dezember 2014 – 8 AZR 1010/13).

Daher ist bei Einwilligungslösungen die Wahrung der Freiwilligkeit besonders zu beachten. Zusätzlich sollte die Einwilligungserklärung sehr deutlich und transparent darstellen, welche Verarbeitungsvorgänge zu welchem Zweck vorgenommen werden sollen. Zweifel an der Freiwilligkeit der Einwilligung dürften hier zu Lasten des Arbeitsgebers ausgehen. Insgesamt sollten Arbeitgeber mit Einwilligungslösungen daher eher sparsam umgehen.

4. Datenverarbeitung auf der Grundlage von Kollektivvereinbarungen

Die DS-GVO benennt explizit Kollektivvereinbarungen als mögliche Rechtsgrundlage und auch § 26 Abs. 4 BDSG-neu enthält Voraussetzungen für die Datenverarbeitung auf Grundlage von Kollektivvereinbarungen. Die Vorschrift legitimiert damit Datenverarbeitungsvorgänge auf Grundlage von Kollektivvereinbarungen. Alle Erlaubnistatbestände müssen angemessene und besondere Schutzmaßnahmen im Sinne des Art. 88 Abs. 2 DS-GVO umfassen. Um angemessene Maßnahmen zu treffen, ist auch hier grundsätzlich eine Interessenabwägung erforderlich. Pauschale Verarbeitungsverbote zu Gunsten der Arbeitnehmer sind genauso unzulässig wie pauschale Einwilligungen in Datenverarbeitungen. Das BAG hat festgestellt, dass sich aus § 75 Abs. 2 Satz 1 BetrVG die Pflicht der Parteien ergibt, dass auch Regelungen in Kollektivvereinbarungen immer einer Verhältnismäßigkeitsprüfung unterliegen (BAG Urt. v. 09.07.2013 – 1 ABR 2/13 (A)).

Arbeitgeber und Betriebsräte sollten daher aktuelle Vereinbarungen darauf kontrollieren, ob sie den neuen Vorschriften genügen. Gegebenenfalls nötige Anpassungen sollten sie zeitnah vornehmen, da die neuen Regelwerke keine Ausnahmeregelungen für bestehende Vereinbarungen vorsehen.

5. Konzernprivileg

Weder die DS-GVO noch das BDSG-neu enthalten ein ausdrückliches Konzernprivileg, sodass Datenübermittlungen in einer Unternehmensgruppe oder einer Gruppe von Unternehmen die eine wirtschaftliche Einheit darstellen, immer eine Rechtsgrundlage benötigen. Erwägungsgrund 48 der DS-GVO erkennt jedoch an, dass die Verarbeitung von Beschäftigtendaten im Konzern durchaus ein berechtigtes Interesse darstellen kann. Gemäß Art. 26 DS-GVO besteht zusätzlich die Möglichkeit, dass verbundene Unternehmen Daten als gemeinsame Verantwortliche verarbeiten. Die teilnehmenden Unternehmen müssen dazu transparent festlegen, wer welche Rechte und Pflichten eines Verantwortlichen wahrnimmt.

III. Aktuelle Rechtsprechung zum Beschäftigtendatenschutz

Der EGMR hat jüngst geurteilt, dass auch im Falle eines Verbotes der privaten Internetnutzung die Verläufe von Chats nicht generell überwacht werden dürfen (EGMR, Urteil v. 05.09.2017, Az.: 61496/08). Eine Überwachung von Arbeitnehmern muss demnach immer verhältnismäßig und zusätzlich an geeignete Verfahrensgarantien gebunden sein. Nach Ansicht des EGMR gehören dazu (Rn. 121.):

- klare und verständliche Hinweise auf die Möglichkeit einer Überwachung;
- angemessene Information des Arbeitnehmers über den Umfang der Überwachung;
- Vortrag legitimer Gründe für die Überwachung des Mitarbeiters durch den Arbeitgeber;
- Überprüfung, ob mildere Maßnahmen den Zweck erfüllt hätten;
- Abwägung der Folgen der Überwachung für den Mitarbeiter sowie eine strikte Zweckbindung der gewonnen Daten;
- geeignete Maßnahmen, um einen unkontrollierten Zugriff, insbesondere ohne Kenntnis des betroffenen Mitarbeiters, auf die Daten zu verhindern.

Das BAG entschied im Juli 2017 in einem ähnlichen Fall über den Einsatz von sogenannten „Keyloggern“ (BAG, Urteil v. 27.07.2017, Az.: 2 AZR 681/16). Eine solche Software darf nach Auffassung des BAG nur bei einem durch konkrete Tatsachen begründeten Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung eingesetzt werden. Der Einsatz solcher Technologien zu präventiven Zwecken, die einen erheblichen Eingriff in das Persönlichkeitsrecht der Mitarbeiter darstellen, sei unverhältnismäßig.

Beide Urteile zeigen, dass es keine starren Voraussetzungen für die Verarbeitung gibt, wie hier im Rahmen einer Überwachung, sondern grundsätzlich eine sorgfältige einzelfallbezogene Prüfung erforderlich ist. Diese Prinzipien gelten unverändert für die DS-GVO sowie das BDSG-neu fort.

IV. Schritte zur Umsetzung der Anforderungen von § 26 BDSG-neu im Unternehmen

Um auch nach Anwendbarkeit der DS-GVO und des BDSG-neu auf der sicheren Seite zu sein, sollten Unternehmen alle internen Datenverarbeitungsvorgänge auf den Prüfstand stellen. Insbesondere sollten die Unternehmen Folgendes prüfen:

- Welche Datenverarbeitungen führen sie derzeit durch und stehen diese im Einklang mit den kommenden Voraussetzungen? Dabei sollte vor allem ein Schwerpunkt auf die Prüfung der Erforderlichkeit der Verarbeitung gelegt werden. ▸

Dies gilt auch für Datenverarbeitungen durch den Betriebsrat. Auch dieser muss sich zukünftig an den Vorgaben der DS-GVO und des BDSG-neu messen lassen.

- Ist der Verantwortliche in der Lage, die sonstigen Rechte und Pflichten aus der DS-GVO zu gewährleisten? Dies gilt insbesondere im Hinblick auf die in Art. 5 DS-GVO festgelegten Datenschutzgrundsätze, wie die Prinzipien der Zweckbindung, Datenminimierung und Transparenz. Der Verantwortliche muss zudem sicherstellen, dass er den Informationspflichten nach der DS-GVO nachkommt und die Betroffenenrechte hinreichend wahrt.
- Anpassung bestehender Betriebsvereinbarungen an die umfassenden Vorgaben der DS-GVO. Künftig müssen die Betriebsparteien sicherstellen, dass Betriebsvereinbarungen angemessene und besondere Schutzmaßnahmen im Sinne des Art. 88 Abs. 2 DS-GVO enthalten. Hierbei sollten Unternehmen auch die Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 DS-GVO im Auge behalten. In der Praxis kommt hier einige Arbeit auf Unternehmen zu.
- Genügen die bestehenden Einwilligungen den neuen Anforderungen oder müssen sie möglicherweise angepasst werden?

V. Fazit

Die neuen Regelungen unterscheiden sich inhaltlich nicht grundsätzlich vom bisherigen Recht. Es kommen allerdings einige neue Anforderungen hinzu. Daher müssen Unternehmen ihre bisherigen Prozesse und Strukturen zum Datenschutz gründlich überprüfen und anpassen. Vor allem wegen sonst drohender Schadenersatzforderungen sowie möglicher Geldbußen von bis zu 20 Mio. Euro (oder bis zu 4 Prozent des globalen Vorjahresumsatzes) sollten Arbeitgeber Anforderungen der DS-GVO sorgfältig und rechtzeitig umsetzen. Eines der wesentlichen Ziele von Projekten zur Umsetzung der DS-GVO muss darin liegen, sich in künftigen Gerichtsverfahren gut gegen Vorwürfe mangelnden Datenschutzes verteidigen zu können. Unternehmen sind daher gut beraten, ihre Dokumentationssysteme zum Datenschutz an den prozessualen Anforderungen künftig drohender Rechtsstreitigkeiten auszurichten.

Über die Autoren

Tim Wybitul
ist Partner bei Hogan Lovells Frankfurt und berät Unternehmen umfassend zum Datenschutz. Der Bundesgerichtshof und das Bundesarbeitsgericht zitierten seine Veröffentlichungen in mehreren Entscheidungen.

Kai Wendt
ist wissenschaftlicher Mitarbeiter bei Hogan Lovells Frankfurt. Er arbeitet an seiner Dissertation am Institut für Rechtsinformatik an der Universität Hannover.

Die Verfasser danken Frau Rechtsanwältin Isabelle Brams, Hogan Lovells International LLP, Frankfurt am Main für ihre wertvollen Anregungen.

▶ http://hoganlovells-blog.de/

Hogan Lovells

SICHERHEIT DER VERARBEITUNG NACH DER EUROPÄISCHEN DATENSCHUTZGRUNDVERORDNUNG. WAS ÄNDERT SICH, WAS BLEIBT?

Helmut Eiermann

Im Rahmen der Vereinheitlichung des europäischen Rechtsrahmens für den Datenschutz ändern sich die Regelungen zu den Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten. Neben einer veränderten Terminologie werden Instrumente wie Risikoanalyse, Sicherheitsmanagement, Verhaltensregeln, Zertifizierung oder Datenschutzfolgeabschätzung vorgegeben. Der Beitrag stellt dar, in welchem Umfang bisherige Vorkehrungen erhalten bleiben können und wo sich Änderungen ergeben.

Sicherheit der Verarbeitung

Die Regelungen der Europäischen Datenschutzgrundverordnung (DS-GVO) zur Sicherheit der Verarbeitung ersetzen die bisherigen technisch-organisatorischen Vorgaben in § 9 Bundesdatenschutzgesetz (BDSG) („10 Gebote"). Die wesentlichen Anforderungen dazu finden sich in den Artikeln 5, 25 und 32. Für die Interpretation relevante Überlegungen sind u.a. den Erwägungsgründen 78, 83, 84 zu entnehmen.

Danach muss durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit gewährleistet werden. Anders als bislang im BDSG wird, wie derzeit bereits in einer Reihe von Landesdatenschutzgesetzen, dabei ausdrücklich insgesamt, d.h. nicht nur bezogen auf Verschlüsselung und Pseudonymisierung, auf den Stand der Technik Bezug genommen. Was unter „Stand der Technik" zu verstehen ist, wird in der Grundverordnung zwar nicht konkretisiert, jedoch ist dieser Begriff nicht gänzlich neu. Letztlich geht es hierbei um technische Maßnahmen, deren Geeignetheit und Effektivität erwiesen ist. Dabei ist dem Begriff „Stand der Technik" implizit, dass es sich jeweils um eine zum aktuellen Zeitpunkt vorgenommene Bewertung handelt, die an technische Entwicklungen und sich neu ergebende Risiken anzupassen ist.

Die an Art und Zweck der Verarbeitung sowie an den Implementierungskosten orientierte Bewertung entspricht weitgehend den bisherigen Verhältnismäßigkeitsüberlegungen und stellt insoweit keinen neuen Ansatz dar. Konkrete Maßnahmen, wie in Form der bisherigen Kontrollen der Anlage zu § 9 BDSG, werden, mit Ausnahme der beiden Datenschutzinstrumente Pseudonymisierung und Verschlüsselung, in Art. 32 Abs. 1 DS-GVO nicht genannt. Damit sind die Vorgaben zunächst abstrakter als bislang.

In der Terminologie verwendet die DS-GVO in Art. 32 jedoch klassische Begriffe der IT-Sicherheit bzw. die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Insoweit kann auf hierfür relevante Systematiken wie die Grundschutzkataloge[1] des Bundesamts für Sicherheit in der ▶

[1] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

Informationstechnik (BSI) daher zunächst auch weiterhin zurückgegriffen werden. Diese geben hinsichtlich der für die jeweiligen IT-Szenarien in Betracht kommender Maßnahmen den Stand der Technik (s.o.) wider.

Auch wenn zu erwarten ist, dass der künftige Europäische Datenschutzausschuss Leitlinien oder Verhaltensregeln zur Konkretisierung der Anforderung an die Sicherheit der Verarbeitung formulieren wird, ist doch davon auszugehen, dass diese sich inhaltlich und methodisch an anerkannten Standards der IT-Sicherheit (z.B. ISO 27001) orientieren, da europäische Gremien wie die ENISA in ihren Empfehlungen ebenfalls auf diese zurückgreifen, die BSI-Empfehlungen auch auf internationaler Ebene Eingang in entsprechende Systematiken gefunden haben (Common Criteria) und die bereits vorhandenen Zertifizierungsmöglichkeiten nach BSI-Grundschutz auch die ISO 27001 einbeziehen. Insoweit ergibt sich hinsichtlich des Baukastens an Maßnahmen die für eine angemessene Sicherheit der Verarbeitung nach Art. 32 DS-GVO zu ergreifen sind, keine grundsätzlich neue Situation. Solange seitens des Europäischen Datenschutzausschusses keine anderweitigen Vorgaben gemacht werden, kann, jedenfalls im Bereich des normalen Schutzbedarfs bzw. eines normalen Risikos, auf die Gefährdungs- und Maßnahmenkataloge des BSI-Grundschutzes zurückgegriffen werden. Um den Anforderungen des Datenschutzes zu genügen, sind über den Aspekt der IT-Sicherheit hinaus weitere Gesichtspunkte in den Blick zu nehmen (s.u.).

Neben den bekannten Begrifflichkeiten aus der IT-Sicherheit verwendet DS-GVO den Begriff der Belastbarkeit (engl. „resilience"). Nähere Angaben, welche Maßnahmen zur Belastbarkeit positiv beitragen, nennt die DS-GVO dazu nicht. Auch wenn in diesem Zusammenhang Aspekte der Widerstandsfähigkeit z.B. gegenüber Angriffen oder der raschen Wiederherstellung nach Beeinträchtigungen des Betriebs eine Rolle spielen dürften, und damit die entsprechenden Schutzmaßnahmen hinsichtlich Verfügbarkeit, Integrität und Vertraulichkeit, bleibt abzuwarten, welche weitergehenden Gesichtspunkte für eine ausreichende Belastbarkeit i.S.d. Grundverordnung künftig zu berücksichtigen sein werden.

Risikoanalyse

Auch wenn im Rahmen der Angemessenheitsbewertung von Datenschutz-Maßnahmen Gefährdungen und Risiken bislang schon in den Blick zu nehmen waren, ergeben sich hier durch die Datenschutzgrundverordnung maßgebliche Änderungen. Von Bedeutung ist künftig ausdrücklich ein (formalisierter) risikobasierter Ansatz, d.h. die Ausrichtung der erforderlichen Maßnahmen an der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken. Dabei sind insbesondere folgende Risiken in den Blick zu nehmen:

- unbeabsichtigte/unrechtmäßige Vernichtung und Veränderung,
- unbeabsichtigter/unrechtmäßiger Verlust,
- unbefugte Offenlegung,
- unbefugter Zugang zu personenbezogenen Daten,
- Wahrnehmung von Betroffenenrechten

Dies begründet die Notwendigkeit einer stärker als bislang formalisierten Risikoanalyse. Die Beurteilung der Risiken für die Rechte und Freiheiten ist ein wesentlicher Teil der Anwendung der DS-GVO. Das für den Datenschutz spezifische Risiko besteht darin, dass in Rechte und Freiheiten Betroffener stärker eingegriffen wird, als es rechtlich zulässig ist. Die DS-GVO benennt in Erwägungsgrund 75 beispielhaft Verarbeitungsvorgänge, die besonders schwer wiegen: die Verarbeitung sensibler Daten sowie die Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte.

Aus den Erwägungsgründen 75 und 94 Satz 2 DS-GVO ergibt sich, dass der Begriff des Risikos für Rechte und Freiheiten natürlicher Personen Beeinträchtigungen bezeichnet, die sich aus einer Verarbeitung ergeben können. Das Risiko muss sowohl aus der Beurteilung

- der Eintrittswahrscheinlichkeit und der Schwere eines möglichen Schadens, als auch
- der Schwere der Beeinträchtigung der Rechte und Freiheiten, die sich aus der Verarbeitung selbst ergibt,

abgeschätzt werden. Beeinträchtigungen sind nur gerechtfertigt, wenn das Risiko so weit wie möglich durch Abhilfemaßnahmen gemindert und begrenzt wird. Weiterhin können Beeinträchtigungen der Rechte und Freiheiten natürlicher Personen Schäden zur Folge haben. Als solche kommen physische, materielle oder immaterielle Schäden in Betracht (Erwägungsgrund 75). Der Schadensbegriff ist somit nicht auf monetäre bzw. materielle Schäden begrenzt. Beispiele möglicher Schäden sind Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile, Erschwerung der Rechtsausübung und Verhinderung der Kontrolle durch betroffene Personen.

Die DS-GVO verwendet die Unterscheidungen „Risiko" (z. B. Erwägungsgrund 76) und „hohes Risiko" (u.a. Art. 35, 36). Daneben findet sich die Formulierung „voraussichtlich nicht zu einem Risiko führend." (Art. 27 Abs. 2 lit. a und Art. 33 Abs. 1 DS-GVO). Da es vollständig risikolose Verarbeitungen nicht geben kann, dürfte die Formulierung „nicht zu einem Risiko führend" so verstanden werden, dass mit der Verarbeitung lediglich geringe Risiken verbunden sind. Ziel der Risikobeurteilung ist es daher, die Risiken nach den Abstufungen „geringes Risiko", „Risiko" und „hohes Risiko" zu bestimmen.

Nach der Auswahl der den Risiken entgegenwirkenden bzw. diese minimierenden Maßnahmen ist das verbleibende Restrisiko abzuschätzen und der Umgang damit zu bestimmen. Ist das Restrisiko tragbar, kann die Verarbeitung durchgeführt werden. Dabei ist zu berücksichtigen, dass sich die Einschätzung des Restrisikos über die Zeit oder durch bestimmte Ereignisse ändern kann und darauf reagiert werden muss. Liegt das Restrisiko im Bereich „hohes Risiko", muss vor Beginn einer Verarbeitung eine Konsultation der Aufsichtsbehörde erfolgen (Art. 36 DS-GVO).

Die Entscheidung, ob ein Restrisiko getragen wird, liegt wie bereits heute beim Verantwortlichen. Er muss genau prüfen (und wegen Art. 5 Abs. 2 DS-GVO als Nachweis für die Aufsichtsbehörde dokumentieren), ob alle ihm nach dem Grundsatz der Verhältnismäßigkeit möglichen Maßnahmen zur Eindämmung des Risikos ergriffen wurden.

Standard Datenschutzmodell

Um den Anforderungen des Datenschutzes zu genügen, sind über den Aspekt der IT-Sicherheit hinaus weitere Gesichtspunkte in den Blick zu nehmen. Bislang ist dies im Baustein 1.5 „Datenschutz"[2] der BSI IT-Grundschutzkataloge dargestellt, der über technisch-organisatorische Punkte hinaus die Zulässigkeit der Datenverarbeitung, die Wahrnehmung der Betroffenenrechte oder die Datensparsamkeit anspricht. Bei der Festlegung der Bereiche, in denen geeignete Schutzmaßnahmen zu treffen sind, sowie für die Risikoanalyse und Datenschutzfolgeabschätzung empfiehlt sich künftig eine Orientierung an dem von der Datenschutzkonferenz entwickelten „Standard Datenschutzmodell"[3].

Dieses beschreibt eine Methodik zur Datenschutzprüfung auf der Basis einheitlicher Gewährleistungsziele. Es fußt auf dem Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. März 2010. Das Modell greift die klassischen Ziele der IT-Sicherheit auf und ergänzt diese um datenschutzbezogene Schutzziele:

- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Transparenz
- Intervenierbarkeit
- Nichtverkettbarkeit
- Prinzip der Datensparsamkeit

Das Standard-Datenschutzmodell orientiert sich methodisch am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik, überführt datenschutzrechtliche Anforderungen in einen Katalog von Gewährleistungszielen, gliedert die betrachteten Verfahren in die Komponenten Daten, IT-Systeme und Prozesse und arbeitet mit drei Schutzbedarfsabstufungen. Es berücksichtigt die grundlegenden Datenschutzprinzipien Zweckbindung, Erforderlichkeit, Wahrnehmung der Betroffenenrechte und Transparenz der Verarbeitung. Ein auf die Gewährleistungsziele abgestimmter Maßnahmenkatalog ist in Vorbereitung. ▸

[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01005.html

[3] https://www.datenschutz.rlp.de/de/themenfelder-themen/standard-datenschutzmodell/

Das Modell gibt eine Methode an die Hand, um mit Hilfe von Schutzzielen rechtliche Datenschutzanforderungen sowie technische und organisatorische Funktionen und Schutzmaßnahmen in ein systematisch bestimmbares Verhältnis zueinander zu setzen. Es ermöglicht den Verantwortlichen, geeignete Maßnahmen zu planen und umzusetzen und fördert damit die datenschutzgerechte Gestaltung von IT-Verfahren. Im Rahmen der in Art. 40 DS-GVO vorgesehenen Verhaltensregeln soll das Standard-Datenschutzmodel von deutscher Seite als Prüfmaßstab bei der Umsetzung der Europäischen Datenschutz-Grundverordnung vorgeschlagen werden.

Datenschutzmanagement

Art. 32 Abs. 1 Buchstabe d) der Grundverordnung schreibt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung vor. Dies bedeutet, dass, ähnlich wie im Bereich der IT-Sicherheit durch ISO 27001 beschrieben, der Verantwortliche ein Datenschutz-Management-System implementieren muss, bei dem im Wege eines regelmäßigen Planungs-, Umsetzungs-, Überprüfungs- und Handlungszyklus Risikoentscheidungen und daraus abgeleitete Schutzmaßnahmen evaluiert und erforderlichenfalls angepasst werden. Methodisch wird man hier, solange auf europäischer Ebene keine anderweitigen Vorgaben gemacht werden, auf die genannte ISO 27001 bzw. die Empfehlungen des BSI-Standards 200-1 zurückgreifen können.

Rechenschafts- und Dokumentationspflicht

Die bisherige Empfehlung der Datenschutzaufsichtsbehörden, Schutzbedarfsfestlegungen und darauf ausgerichtete Maßnahmen in einem Sicherheitskonzept zu dokumentieren, erhält durch Art. 5 Abs. 2 DS-GVO künftig eine ausdrückliche rechtliche Grundlage. Danach muss der Verantwortliche die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DS-GVO, d.h. u.a. die Rechtmäßigkeit der Verarbeitung, Zweckbindung, Datenminimierung sowie eine angemessene Sicherheit der Verarbeitung nachweisen können („Rechenschaftspflicht“). Dies erfordert eine prüfbare verfahrensbezogene Dokumentation. Mit Blick auf die Privilegierung nach Art. 32 Abs. 3 DS-GVO, bzw. den damit leichter zu führenden Nachweis der Datenschutzkonformität, werden künftig genehmigte Verhaltensregeln ebenso wie Zertifizierungen an Bedeutung gewinnen und vorhandene Ansätze (z.B. Code of Conduct der Versicherungswirtschaft) fortführen. Hierfür darf vermutet werden, dass sich Zertifizierungsverfahren und -kriterien an den Vorgaben des seinerzeit von der Europäischen Union im Rahmen des eTEN-Programms geförderten Europäischen Datenschutzgütesiegels „European Privacy Seal - EuroPrise“ orientieren.

Über den Autor

Helmut Eiermann
ist stellvertretender Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz und Leiter des dortigen Bereichs Technik.

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

VORGEHEN BEI DATENSCHUTZ-FOLGENABSCHÄTZUNGEN

Dr. Michael Friedewald und Dr. Nicholas Martin

Die EU Datenschutz-Grundverordnung (DS-GVO) schreibt in bestimmten Fällen eine Datenschutz-Folgenabschätzung (DSFA) vor. Sie löst die bisherige Vorabkontrolle ab. Da Verstöße gegen den die DSFA regelnden Art. 35 DS-GVO mit Geldbußen von bis zu €10 Millionen oder 2% des Jahresumsatzes belegt werden können, ist die Pflicht zur DSFA ernst zu nehmen. Dieser Aufsatz gibt Hilfestellung.

Was ist eine DSFA und wann ist sie erforderlich?

Die DSFA ist ein Prozess um Risiken für Rechte und Freiheiten natürlicher Personen, die aus Verarbeitungen personenbezogener Daten entstehen, zu identifizieren, zu bewerten und einzudämmen. Sie ist durchzuführen wenn Art, Umfang, Umstände und Zwecke einer Verarbeitung „voraussichtlich“ zu einem „hohen Risiko“ für Rechte und Freiheiten natürlicher Personen führen (Art. 35 Abs. 1 DS-GVO). Zu beachten ist, dass die DS-GVO nicht abschließend festlegt, wann von einem „hohen Risiko“ auszugehen ist. Als Orientierungshilfe werden nur Regelbeispiele genannt. Für die Datenschutzpraxis bedeutet dies, dass Prozesse innerhalb des Projekt- und Risiko-Managements etabliert werden sollten um verlässlich zu bewerten, ob eine DSFA nötig ist. Um Fahrlässigkeitsvorwürfe zu vermeiden, sollten gerade bei Entscheidungen gegen die Durchführung einer DSFA die Gründe hierfür dokumentiert werden. Unter Umständen entfällt die Pflicht zur DSFA auch bei Verarbeitungen mit hohem Risiko (hierzu Art. 35 Abs. 10).

Die Rechtspflicht, bei Verarbeitungen mit voraussichtlich hohem Risiko eine DSFA durchzuführen, gilt auch für Verarbeitungen, die bereits vor Mai 2018 begonnen wurden. Eine Ausnahme bilden Verarbeitungen, die bereits von einer Datenschutz-Aufsichtsbehörde im Rahmen der Vorabkontrolle (prior checking) geprüft wurden. Hier hat die Artikel-29 Datenschutzgruppe festgelegt, dass die Verarbeitung auch ab Mai 2018 ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

weiterbetrieben werden darf, vorausgesetzt, dass sie seit der Vorabkontrolle nicht verändert wurde.

Hohes Risiko

Zur Erkennung eines wahrscheinlich hohen Risikos hat der Verantwortliche drei Entscheidungshilfen zur Orientierung: die Regelbeispiele der DS-GVO, eine von den Aufsichtsbehörden noch zu erstellende Muss-Liste und die Stellungnahme der Artikel-29 Gruppe zur Risikoerkennung.[1]

Von zentraler Bedeutung ist, dass die Risikobetrachtung aus Perspektive der betroffenen Personen erfolgt, nicht aus der der Organisation wie im Fall der IT-Sicherheit. Die Risiken, die die DSFA aufdecken soll, können ebenso aus bestimmungsgemäßem Handeln der Organisation wie aus Angriffen Unbefugter hervorgehen. Zudem zielt die DSFA auf den Grundrechtsschutz ab. Risiken dürfen daher nicht anhand der Zahl der Betroffenen oder möglicher finanzieller Risiken für die Organisation bewertet werden, sondern nur anhand von Schwere und Eintrittsrisiko für den Einzelnen.

Regelbeispiele in der DS-GVO

Art. 35 Abs. 3 führt drei Fälle an, die eine DSFA erforderlich machen:

- Systematische umfassende, auf automatisierter Verarbeitung gründende Bewertung persönlicher Aspekte natürlicher Personen, die rechtswirksam ist oder Personen erheblich beeinträchtigt (z.B. Scoring, Profiling, automatisierte Einzelentscheidungen)
- Umfangreiche Verarbeitungen besonderer personenbezogener Daten nach Art. 9 Abs. 1 (z.B. ethnische Herkunft) oder Daten über Verurteilungen und Straftaten nach Art. 10
- Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche
- Auch die Verwendung neuer Technologien legt nach Art. 35 Abs. 1 das Vorliegen hoher Risiken nahe.

Muss-Liste der Aufsichtsbehörden

Art. 35 Abs. 4 verpflichtet die Aufsichtsbehörden, Listen mit Verarbeitungen zu erstellen, die eine DSFA erfordern. Diese Listen befinden sich noch in Bearbeitung. Die Behörden sind auch ermächtigt, Listen mit Verarbeitungen, die keine DSFA benötigen, zu veröffentlichen. Es ist aber unwahrscheinlich, dass sie hiervon Gebrauch machen werden.

Kriterien der Artikel-29 Gruppe

Die Artikel-29 Gruppe hat eine Stellungnahme mit Kriterien vorgelegt, die auf hohe Risiken hindeuten.[2] Hierzu zählen Bewertung, Scoring, Prognosen und Profiling; automatisierte Entscheidungen; systematische Überwachung; sensible Daten; umfangreiche Datenmengen; Kombination von Datensätzen; Daten Schutzbedürftiger; Einsatz innovativer Technologien oder Organisationsformen; und Verarbeitungen, die verhindern, dass Personen Rechte ausüben, Dienstleistungen beanspruchen oder Verträge abschließen können.

Liegt keines der genannten Kriterien vor, muss der Verantwortliche allgemein prüfen, ob ein hohes Risiko aus der geplanten Verarbeitung entstehen könnte.

Rolle des Datenschutzbeauftragten

Die Durchführung der DSFA ist laut Art. 35 Abs. 1 die Aufgabe des Verantwortlichen. Die Aufgaben des Datenschutzbeauftragten (DSB) bei der DSFA beschränken sich nach Art. 39 Abs. 1 DS-GVO auf die Beratung des Verantwortlichen – letzterer ist verpflichtet, diesen Rat einzuholen – und auf die Überwachung ihrer Durchführung. Ferner ist er Anlaufstelle für die Aufsichtsbehörde (Art. 39 Abs. 1), etwa im Rahmen der vorherigen Konsultation nach Art. 36 DS-GVO. Wie Laue u.a. ausführen, zwingt das dem DSB u.U. einen schwierigen Spagat auf: er muss den Verantwortlichen beraten, aber die Aufsichtsbehörden ev. auch über vom Verantwortlichen nicht beachtete Empfehlungen informieren.[3]

In der Praxis dürfte dem DSB eine große Rolle bei der Durchführung der DSFA zukommen. Unklar ist, ob er selber die DSFA durchführen sollte. Zwar kann der Verantwortliche die Durchführung an Dritte delegieren, einer Delegation an den DSB steht aber dessen Weisungsunabhängigkeit und Pflicht, die Durchführung zu überwachen, entgegen. Schließlich kann er sich schlecht selbst überwachen. Andererseits dürfte es kleinen Organisationen schwer fallen, intern neben dem DSB weitere Datenschutzexperten für die DSFA zu benennen. Die Stellungnahme der Artikel-29 Gruppe zum DSB löst dieses Problem insofern, als dass sie die Breite seiner Beratungsbefugnis betont. Fragen, zu denen der Verantwortliche den DSB konsultieren soll, sind u.a. ob eine DSFA nötig ist und korrekt durchgeführt wurde sowie welche DSFA-Methode und Schutzmaßnahmen zu wählen sind. Wo der Verantwortliche dem Rat des DSB widerspricht soll er dies schriftlich begründen.[4] Praktisch kommt dies der Durchführung der DSFA durch den DSB nahe. Eine persönliche Haftung des DSB für die Durchführung einer DSFA und die Richtigkeit der Ergebnisse besteht nicht.

DSFA Prozess

Die DS-GVO definiert keinen Prozess für die Durchführung einer DSFA. Art. 35 legt nur fest, dass sie vor Beginn der Verarbeitung erfolgen und mindestens Folgendes beinhalten muss:

- eine systematische Beschreibung der Verarbeitung, ihrer Zwecke und ggf. der berechtigten Interessen des Verantwortlichen,
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck,
- eine Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen und
- die zur Bewältigung der Risiken geplanten Maßnahmen inklusive Nachweis, dass die Verordnung eingehalten wird.

Der vom „Forum Privatheit" entwickelte DSFA-Prozess erfüllt diese Anforderungen. Er gliedert sich in fünf – hier verkürzt dargestellte – Phasen.[5] Der Prozess ist hier linear beschrieben, in der Praxis ist es aber u.U. nötig, einzelne Schritte wiederholt zu durchlaufen.

1 Vorbereitungsphase

Zuerst wird die Relevanzschwelle geprüft: Muss eine DSFA durchgeführt werden? Diese Entscheidung soll anhand der besprochen Entscheidungshilfen erfolgen und dokumentiert werden.

Als nächstes wird ein geeignetes Team zusammengestellt. Dieses sollte eine Mischung aus technischer, juristischer und betriebswirtschaftlicher Expertise beinhalten, und die für die Verarbeitungsvorgänge verantwortliche Geschäftseinheit einbinden.

Dann ist der Prüfgegenstand zu beschreiben. Dies beinhaltet erstens die Verarbeitungsverfahren, inkl. verwendeter Daten, deren Formate, IT-Systeme, Schnittstellen, Prozesse und Funktionsrollen. Dabei kann auf den bereits existierenden Verfahrensverzeichnissen aufgebaut werden. Ein Datenflussdiagramm ist hierfür hilfreich. Zweitens ist der Zweck der Verarbeitung zu definieren, und ihre Notwendigkeit im Hinblick auf den Zweck zu bewerten: Steht die Verarbeitung im Verhältnis zum Zweck oder kann dieser auch mit weniger grundrechtsinvasiven Verfahren erzielt werden?

Darauf folgt die Identifikation der Akteure und betroffenen Personen. Diese umfassen alle, die das Verfahren beeinflussen können sowie Personen, die mittel- oder unmittelbar von der Verarbeitung betroffen sind. Je nach Anwendung können z.B. Kunden, Mitarbeiter, Patienten oder unbeteiligte Passanten betroffene Personen sein.

Im letzten Schritt wird die maßgeblichen Rechtsgrundlage (z.B. EU-Recht, nationale Gesetze wie Sozialgesetz) und der Erlaubnistatbestand (z.B. Einwilligung, berechtigte Interessen) auf der die Verarbeitung beruht, identifiziert. So kann der Verantwortliche die Rechtmäßigkeit der Verarbeitung nachweisen.

Die Ergebnisse der Vorbereitungsphase sollten dokumentiert und vom Verantwortlichen als verbindlich bestätigt werden.

Danach kann ggf. eine Betroffenen-Konsultation nach Art. 35 Abs. 9 erfolgen. Diese ist nicht zwingend vorgeschrieben und wird vermutlich eher die Ausnahme bleiben. Jedoch ist der Verantwortliche geraten, bei der DSFA zumindest die organisationsinternen Stellen zu konsultieren, die den engsten Kontakt zu den Betroffenen haben, z.B. Betriebsrat oder Verkaufsabteilung.

▶

[1] Artikel-29-Datenschutzgruppe (2017). Guidelines on Data Protection Impact Assessments (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679. 17/EN, WP 248. http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[2] Laue, P. u.a. (2016): Das Neue Datenschutzrecht in der betrieblichen Praxis. Baden-Baden: Nomos. S. 209

[4] Artikel-29-Datenschutzgruppe (2016). Guidelines on Data Protection Officers (DPOs). Working Paper 16/EN, WP 243. http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

[5] Eine vollständige Darstellung findet sich in Friedewald, M. u.a. (2017): Datenschutz-Folgenabschätzung. Werkzeug für einen besseren Datenschutz. 3. Auflage. In Bearbeitung.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

2 Bewertungsphase

Erster Schritt der Bewertungsphase ist die *Identifikation der Schutzziele*. Das Standard-Datenschutzmodell (SDM) der Datenschutzkonferenz[6] schlägt sechs Schutzziele vor: Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, und Intervenierbarkeit sowie Datensparsamkeit.

Daran schließt sich die *Identifikation möglicher Angreifer, Angriffsmotive und -ziele* an. Hier muss die Betroffenen- und nicht die Organisationsperspektive eingenommen werden. Zu schützen sind Rechte und Freiheiten der Betroffenen – nicht die Organisationsinteressen. Angreifer sind nicht nur unbefugte Dritte, sondern in erster Linie regelkonform handelnde interne und externe Stellen (z.B. Behörden, andere Unternehmen). Risiken entstehen oft aus illegitimen Überdehnungen des Zwecks durch den Betreiber selbst oder durch Anfragen dritter Stellen. Die mit der Durchführung der DSFA Betrauten müssen hierfür sensibilisiert werden. Dem Datenschutzbeauftragten kommt dabei eine wichtige Rolle zu.

Anschließend sind das Risiko zu bewerten und der Schutzbedarf zu ermitteln. Grundsätzlich richtet sich das Risiko nach der möglichen Schadensgröße und ihrer Eintrittswahrscheinlichkeit. Schadensgröße und Schutzbedarf wiederum hängen von der Sensitivität der Daten (Eingriffsintensität) und der Tragweite der Entscheidungen, die auf Basis der Verarbeitung getroffen werden können, ab. Schäden können physischer, materieller und immaterieller Natur sein, z.B. Identitätsdiebstahl, Diskriminierung und andere gesellschaftliche Nachteile (Erwägungsgrund 75 DS-GVO).

Meist sind weder Schadensgröße noch Eintrittswahrscheinlich seriös quantifizierbar. Auf Pseudo-Berechnungen sollte daher verzichtet und die Risikobewertungsformel Risko = Schadensgröße x Wahrscheinlichkeit nur als Heuristik betrachtet werden. Stattdessen sollte der Verantwortliche eine nachvollziehbare Argumentation für die Risikobewertung anhand der Angriffsszenarien und Schutzzielanforderungen vorlegen.

[6] Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder (2016): Das Standard-Datenschutzmodell. https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf.

3 Maßnahmenphase

Auf Basis der Risikobewertung sind passende Schutzmaßnahmen zu *identifizieren* und *umzusetzen*. Der Arbeitskreis Technik der Datenschutzkonferenz hat 2016 den Entwurf eines Referenzmaßnahmenkatalogs vorgelegt, der Schutzmaßnahmen für jedes Schutzziel im SDM definiert. Dieser Katalog wird aktuell überarbeitet. Wichtig ist, ihn nicht als abzuhakende Checkliste zu verwenden. Stattdessen sind Verarbeitung und Schutzziele samt Wechselwirkungen in ihrer Gesamtheit zu betrachten. Um eine verlässliche Implementierung zu gewährleisten sollten entsprechende Prozesse im Projekt-Management festgeschrieben werden.

Maßnahmen sind auf ihre Wirksamkeit zu testen. Es sind u.U. mehrere Maßnahmen vorzusehen, um das Risiko auf ein akzeptables Niveau zu senken. Die Tests, Bewertungsergebnisse und ev. Restrisiken sind zu dokumentieren. Wenn hohe Restrisiken verbleiben, die nicht durch Maßnahmen eindämmbar sind, darf die Verarbeitung nicht freigegeben werden. In diesem Fall ist nach Art. 36 Abs. 1 DS-GVO die Aufsichtsbehörde zu konsultieren.

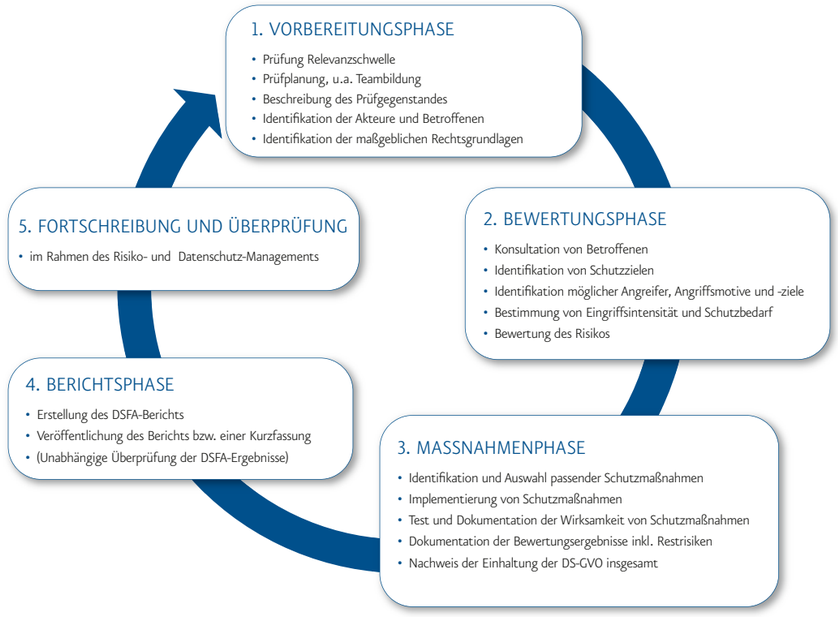
Schließlich ist nachzuweisen, dass die Verarbeitung die DS-GVO einhält. Die angefertigte Dokumentation der Verarbeitungsvorgänge, Risiken und Maßnahmen bilden dabei die Grundlage für den DSFA-Bericht.

4 Berichtsphase

Der DSFA-Bericht ist auf Verlangen der Aufsichtsbehörde vorzulegen. Eine Veröffentlichung des Berichts ist nicht vorgeschrieben, wird aber empfohlen. Technische und Geschäftsgeheimnisse können dabei gekürzt, negative Details sollten aber nicht verschwiegen werden.

5 Fortschreibung und Überprüfung

Die DSFA ist kein einmaliger Prozess. Im Gegenteil sind technische, organisatorische und andere Rahmenbedingungen der Verarbeitung während des Lebenszyklus des Projekts zu überwachen, und die DSFA ggf. zu wiederholen, falls Änderungen auf neue Datenschutzrisiken hindeuten. Auch ist zu beobachten, ob die Schutzmaßnahmen greifen, oder andere gewählt werden müssen. Diese Fortschreibung der DSFA ist von Art. 35 Abs. 11 mandatiert. Eine Einbindung der DSFA in das allgemeine Datenschutz- und Risiko-Management ist daher empfehlenswert.



Weiterentwicklung des DSFA Prozesses

Zur Weiterentwicklung des DSFA Prozesses wird das Fraunhofer ISI im kommenden Jahr Tests des besprochenen Prozesses in Unternehmen und Behörden durchführen. Hierdurch soll der Erfahrungsaustausch mit Praktikern forciert werden. Für Unternehmen und Behördenstellen bestehen auch Möglichkeiten, als Test-Partner in das Projekt aufgenommen zu werden. Bei diesen würden Teile des DSFA Prozesses unter Expertenbegleitung praktisch erprobt werden. Kooperationspartner im BMBF-geförderten Projekt sind die FH Kiel und das Leibnitz Institut für Informationsinfrastruktur. Weitere Informationen sind auf der Projekt-Webseite erhältlich:

www.dsfa.eu

Über die Autoren

Dr. Michael Friedewald
Geschäftsfeldleiter IKT im Competence Center Neue Technologien, Fraunhofer Institut für System- und Innovationsforschung (ISI)

Dr. Nicholas Martin
Wissenschaftlicher Mitarbeiter im Competence Center Neue Technologien, Fraunhofer Institut für System- und Innovationsforschung (ISI)

▶ www.isi.fraunhofer.de

Fraunhofer ISI

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

RECHT AUF LÖSCHUNG: DER RADIERGUMMI DER DS-GVO

Tilman M. Dralle, LL.M.

I. Einleitung

Das in Art. 17 der EU-Datenschutz-Grundverordnung („DS-GVO") normierte „Recht auf Löschung" ist vom Grundsatz her nicht neu. Dass personenbezogene Daten nach einer bestimmten Vorhaltefrist zu löschen sind, ist bereits de lege lata so. Aus der datenschutzrechtlichen Praxis ist jedoch zu berichten, dass insbesondere in puncto Löschen gesetzliche Norm und gelebte Realität stark auseinanderfallen. Um es prägnant zu fassen: Deutsche Unternehmen löschen ihre Datenbestände in der Regel nicht oder nur sehr punktuell; Automatisierte Löschroutinen bilden die absolute Ausnahme. Da die fehlende bzw. mangelhafte Umsetzung der DS-GVO-Löschpflichten zukünftig mit einem Bußgeld in Höhe von bis zu 4% des gesamten, weltweit erzielten Vorjahresumsatzes geahndet werden kann[1], hat das Thema inzwischen eine ganz eigene Brisanz entwickelt. Vor diesem Hintergrund soll im Folgenden ein Blick auf die mit Art. 17 DS-GVO verbundenen Herausforderungen geworfen werden.

II. Die Regelung in Art. 17 DS-GVO

Die dreigliedrige Struktur des Art. 17 DS-GVO ist relativ übersichtlich. In Absatz 1 werden sechs Löschgründe definiert, bei deren Vorliegen die Löschpflicht grundsätzlich greift. In Absatz 2 wird das – in letzter Zeit häufig diskutierte, aber in der Praxis für wenige Unternehmen tatsächlich relevante – „Recht auf Vergessenwerden" statuiert, das bei einer Veröffentlichung personenbezogener Daten eine Pflicht zur Information anderer Verantwortlicher über das Löschbegehren beinhaltet. Schlussendlich werden in Absatz 3 fünf Ausnahmen von der Lösch- bzw. Informationspflicht genannt. Die vorliegende Betrachtung exkludiert das „Recht auf Vergessenwerden", da – wie in der Literatur erkannt – die „eigentliche Bedeutung des Art. 17"[2] in der Regelung der klassischen Löschpflichten liegt.

Die sechs Löschgründe in Art. 17 Abs. 1 DS-GVO können wie folgt zusammengefasst werden: Entfall der Notwendigkeit zur Zweckerfüllung (lit. a), Widerruf der Einwilligung (lit. b), Widerspruch gegen die Verarbeitung (lit. c), Unrechtmäßigkeit der Verarbeitung (lit. d), Bestehen einer anderweitigen Rechtspflicht zur Löschung (lit. e), Erhebung personenbezogener Daten eines Kindes in Bezug auf angebotene Dienste der Informationsgesellschaft (lit. f). In diesen Fällen muss unverzüglich, d.h. ohne schuldhaftes Zögern, und unentgeltlich gelöscht werden. Wichtig ist hierbei, dass das „Recht auf Löschung" im Unterschied zu anderen Betroffenenrechten nicht nur durch einen Antrag der betroffenen Person geltend gemacht werden kann, sondern dass parallel dazu eine antragsunabhängige Pflicht des Verantwortlichen zur Löschung besteht („… und der Verantwortliche ist verpflichtet […] zu löschen …").[3]

III. Was verlangt ein „Löschen" nach der DS-GVO?

Was müssen Unternehmen tun, um DS-GVO-konform zu löschen? Die DS-GVO bietet im Gegensatz zum jetzigen BDSG[4] keine Legaldefinition. Es kann jedoch mit einiger Sicherheit davon ausgegangen werden, dass personenbezogene Daten unkenntlich gemacht werden müssen, um den Anforderungen der DS-GVO zu entsprechen. Das bedeutet, dass weder organisatorische Maßnahmen (wie z.B. eine Arbeitsanweisung, dass bestimmte Informationen nicht wahrgenommen werden dürfen)[5] noch „Hinweise[], die kennzeichnen, dass ein Text nicht mehr gelten soll"[6] ausreichend sind. Für die Bewertung der Effektivität technischer Löschmechanismen z.B. auf Festplatten können Standards wie DIN 66399, NIST SP 800-88 und CSEC 2006 herangezogen werden.

IV. Fehlender Einwand der Unverhältnismäßigkeit

Im Gegensatz zum Status Quo[7] kennt die DS-GVO keinen Einwand der Unverhältnismäßigkeit.[8] Bei Vorliegen der entsprechenden Voraussetzungen verlangt Art. 17 auch dann die Löschung, wenn diese mit einem unverhältnismäßig hohen Aufwand einhergeht. Daher können sich die datenverarbeitenden Anwender von Hard- und Software nicht (mehr) darauf berufen, dass eine (Teil-)Löschung aus systemtechnischen Gründen nicht möglich ist. Zwar hatte die deutsche Bundesregierung ursprünglich geplant, den im BDSG verankerten Einwand der Unverhältnismäßigkeit durch das „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU" (DSAnpUG-EU) in die „DS-GVO-Welt" hinüberzuretten.[9] Diese geplante Ausnahme vom Löschgebot war von der Wirtschaft erwartungsgemäß begrüßt worden,[10] sah sich andererseits aber auch heftiger Kritik und dem Verdacht der Unionsrechtswidrigkeit ausgesetzt.[11] Sie wurde in der Folge durch einen Änderungsantrag der Regierungsfraktionen[12] auf Fälle nicht-automatisierter Datenverarbeitungen beschränkt (z.B. Papier-Archive, Mikrofiche). In der Konsequenz müssen datenverarbeitende Unternehmen frühzeitig Druck auf die Hersteller und Anbieter von Hard- und Software ausüben, um – auch im Sinne der „Privacy by Design"-Anforderungen – ab dem 25.5.2018 datenschutzgerechte IT-Technik im Einsatz zu haben.

V. Löschpflicht bei Datensicherungen?

Die Reichweite der Löschverpflichtung aus Art. 17 DS-GVO ist, abgesehen von den in Absatz 3 definierten Ausnahmetatbeständen, nicht a priori beschränkt. Das bedeutet, dass eine Löschung grundsätzlich auf allen Datenträgern zu erfolgen hat. Vor diesem Hintergrund wird in der Literatur teilweise angenommen, dass sich die Löschverpflichtung auch auf Sicherheitskopien (Backups) erstreckt.[13] Folglich müssten Datenlöschungen auch auf Tages-, Wochen- und Monatssicherungen durchgeführt werden, und das selbst dann, wenn es sich lediglich um einzelne Datensätze handelt.[14] Allerdings ist in diesem Zusammenhang auch Art. 32 DS-GVO („Sicherheit der Verarbeitung") zu betrachten, ▸

[1] Siehe Art. 83 Abs. 5 lit. b DS-GVO.

[2] Kühling/Buchner, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 1.

[3] Paal/Pauly, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 20.

[4] § 3 Abs. 4 S. 2 Nr. 5 BDSG.

[5] Kühling/Buchner, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 40.

[6] So aber wohl Gola, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 8.

[7] § 35 Abs. 3 Nr. 3 BDSG.

[8] Siehe hierzu insbesondere Gola, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 31.

[9] Siehe Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Drucksache 18/11325, S. 35.

[10] Siehe Stellungnahme des Gesamtverbandes der Deutschen Versicherungswirtschaft zum DSAnpUG-EU vom 14.2.2017, S. 10-11; Stellungnahme Die Deutsche Kreditwirtschaft zum DSAnpUG-EU vom 20.2.2017, S. 12.

[11] Siehe bspw. Stellungnahme der EAID zum DSAnpUG-EU vom 22.2.2017, Ziff. 1.6; Stellungnahme Dr. Piltz zum DSAnpUG-EU vom 22.3.2017, S. 30; Stellungnahme des Verbraucherzentrale Bundesverbands e.V. zum DSAnpUG-EU vom 13.2.2017, Ziff. 3.6.

[12] Änderungsantrag der Fraktionen der CDU/CSU und der SPD zu dem Gesetzentwurf der Bundesregierung – Drucksache 18/11325, A-Drs. 18(4)842, S. 3.

[13] So Ehmann/Selmayr, Datenschutz-Grundverordnung, EU-DS-GVO Art. 17 Rn. 34; Kühling/Buchner, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 42.

[14] Siehe hierzu die Stellungnahme der GDD zum DSAnpUG-EU vom 22.3.2017, S. 4.

der den Verantwortlichen u.a. dazu verpflichtet, die Verfügbarkeit der Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können (Abs. 1 lit. c). Ein Sicherungs- und Wiederherstellungs-Konzept, das diesen Anforderungen genügt, kann nach hier vertretener Auffassung nur umgesetzt werden, wenn für die gemischten (!) Datenbestände in Backups akzeptiert wird, dass die Regellöschfristen zumindest teilweise überschritten werden.[15] Dabei ist klar, dass die Überschreitung der Regellöschfristen auf das absolut notwendige Maß reduziert werden muss und dass bei einer etwaigen Wiederherstellung diejenigen Daten gelöscht werden müssen, deren Löschfrist bereits abgelaufen ist. So können die Löschpflichten aus Art. 17 DS-GVO und die Datensicherungspflichten gemäß Art. 32 DS-GVO in einen angemessen Ausgleich gebracht werden.

VI. Löschpflichten bei Werbewiderspruch

Eine weitere Herausforderung im Bereich des Rechts auf Löschung in Art. 17 DS-GVO ergibt sich im Zusammenhang mit personenbezogenen Daten, die auch für Direktwerbung verarbeitet werden. Nach Art. 17 Abs. 1 lit. c DS-GVO ist der Verantwortliche verpflichtet, personenbezogene Daten zu löschen, sofern die betroffene Person gemäß Art. 21 Abs. 2 DS-GVO Widerspruch gegen eine Verarbeitung zu Zwecken der Direktwerbung einlegt. Diese Löschverpflichtung ist nicht weiter qualifiziert. Sie erfasst mithin auch solche Fälle, in denen eine Rechtsgrundlage für die Verarbeitung der betreffenden Daten zu anderen Zwecken vorliegt. Art. 21 Abs. 2 und 3 DS-GVO sehen hingegen ein Verarbeitungsverbot nur für Zwecke der Direktwerbung vor. Eine Verarbeitung zu anderen Zwecken ist damit weiterhin erlaubt. Entgegen einer prominenten Literaturmeinung[16] wird hier der Standpunkt vertreten, dass die DS-GVO-Löschpflicht im Fall eines Werbewiderspruchs nicht dahingehend ausgelegt werden kann, dass Daten gelöscht werden müssen, obwohl für ihre Verarbeitung zu anderen als zu Direktwerbezwecken (z.B. zur Vertragserfüllung) eine ordentliche Rechtsgrundlage (z.B. Art. 6 Abs. 1 lit. b DS-GVO) besteht. Falls die Daten, die zu Werbezwecken verarbeitet werden, in einer eigenständigen, separaten Datenverkörperung vorliegen, sind sie selbstverständlich zu löschen.

VII. Rechtsunsicherheit bei Ausnahmetatbeständen

Zusätzlich zu den in Art. 17 Abs. 3 DS-GVO normierten Ausnahmetatbeständen wurden durch den deutschen Gesetzgeber unter Ausnutzung der entsprechenden Öffnungsklausel in Art. 23 DS-GVO weitere Ausnahmen vom Recht auf Löschung durch das DSAnpUG-EU[17] definiert. Eine zentrale Ausnahme, die sich ab dem 25.5.2018 in § 35 Abs. 3 BDSG-neu wiederfinden wird, sieht vor, dass personenbezogene Daten trotz Zweckverbrauchs dann nicht gelöscht werden müssen, wenn entgegenstehende satzungsmäßige oder vertragliche Aufbewahrungsfristen existieren. An die Stelle einer Löschung tritt in einem solchen Fall die Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO. Die Ausnahmevorschrift in § 35 Abs. 3 BDSG-neu begegnet jedoch unionsrechtlichen Bedenken. Zunächst sind satzungsmäßige oder vertragliche Aufbewahrungsfristen keine „rechtlichen Verpflichtungen" i.S.v. Art. 17 Abs. 3 lit. b DS-GVO, da es sich hierbei nicht um „Rechtspflichten des objektiven Rechts",[18] sondern um selbst geschaffene bzw. privatautonom mit Dritten eingegangene Rechtsbindungen handelt. [19] Darüber hinaus ist nicht ersichtlich, wie die Ausnahmevorschrift über die Öffnungsklausel in Art. 23 DS-GVO gerechtfertigt werden könnte. [20] Vor diesem Hintergrund müssen Unternehmen, die sich auf satzungsmäßige oder vertragliche Aufbewahrungsfristen berufen möchten, bis zu einer etwaigen Entscheidung durch den EuGH mit einer gewissen Rechtsunsicherheit leben.

VIII. Informationspflichten, Auskunftsrecht und Verzeichnis von Verarbeitungstätigkeiten: Angabe der Speicherdauer „falls möglich"

Zuletzt soll ein Blick auf die Informationspflichten, das Auskunftsrecht sowie das Verzeichnis von Verarbeitungstätigkeiten im Kontext des Rechts auf Löschung geworfen werden. Nach Art. 13 und 14 DS-GVO muss der Verantwortliche die betroffene Person u.a. über die „Dauer, für die die personenbezogenen Daten gespeichert werden" oder – „falls dies nicht möglich ist" – über die „Kriterien für die Festlegung dieser Dauer" informieren. Das Auskunftsrecht nach Art. 15 sowie das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO verlangen eine Angabe der Speicherdauer respektive Löschfristen ebenfalls nur „falls möglich" bzw. „wenn möglich". Diese einschränkenden Formulierungen sollten jedoch nicht darüber hinwegtäuschen, dass zumindest eine Angabe der *Kriterien* für die Bestimmung der Speicherdauer zwingend vorgeschrieben wird. Unklar ist dabei allerdings, wie diese Transparenzanforderung auszulegen ist. Auf der einen Seite könnten die Kriterien sehr generisch über eine einfache Bezugnahme auf das Gesetz („… nach den gesetzlichen Vorschriften der DS-GVO …") oder die Norm („… nach Art. 17 DS-GVO …") bezeichnet werden.[21] Auf der anderen Seite könnte von den Aufsichtsbehörden gefordert werden, für jede Datenkategorie eine Standardlöschfrist (z.B. 10 Jahre) sowie einen abstrakten Startzeitpunkt (z.B. Ende des Vertragsverhältnisses) zu benennen. Ungeachtet dieser Auslegungsspielräume steht fest, dass Unternehmen ein detailliertes Löschkonzept erarbeiten und damit die Regellöschfristen aller von ihnen verarbeiteten personenbezogenen Daten kennen müssen. Denn nur so können sie der DS-GVO-Rechenschaftspflicht genügen, die vom Verantwortlichen einen Nachweis darüber verlangt, dass die Verarbeitung – und damit auch die Löschung – personenbezogener Daten DS-GVO-konform erfolgt.[22]

IX. Fazit

Die vorstehende Betrachtung zu Art. 17 DS-GVO hat eines gezeigt: Die Anwendung des Rechts auf Löschung birgt für datenverarbeitende Unternehmen sowie für alle, die sich professionell mit Datenschutz beschäftigen, echte Herausforderungen. Zunächst sind da Herausforderungen bei der Auslegung der Löschverpflichtungen (Kapitel III, V, VI, VIII): Was verlangt ein „Löschen" nach der DS-GVO? Gibt es eine unverzügliche Pflicht zur Löschung auch auf Backups? Müssen personenbezogene Daten bei einem Werbewiderspruch gelöscht werden, obwohl diese Daten auch zu anderen als zu Direktwerbezwecken verarbeitet werden? Und: Wie exakt müssen Speicherdauer bzw. Löschfristen im Rahmen der Transparenzpflichten angegeben werden? Zudem gibt es Herausforderungen mit Blick auf die Vereinbarkeit mit EU-Recht (Kapitel VII): Sind die im BDSG-neu enthaltenen Ausnahmen vom Recht auf Löschung mit der DS-GVO kompatibel? Schließlich wurden praktische Herausforderungen bei der Umsetzung des Rechts auf Löschung aufgezeigt (Kapitel IV): Wie soll damit umgegangen werden, dass Art. 17 DS-GVO keinen Einwand der Unverhältnismäßigkeit kennt? Der vorliegende Beitrag hatte zum Ziel, auf diese Fragen erste Antworten zu geben.

Über den Autor

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

Security Consultant mit Schwerpunkt im Bereich Informationssicherheit und Datenschutz, TÜV Rheinland i-sec GmbH

TÜVRheinland®
Genau. Richtig.

[15] Siehe auch DIN 66398:2016-05, Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten, Ziff. 6.3.5 (ohne Bezug auf die DS-GVO).

[16] Kühling/Buchner, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 27.

[17] BGBl. 2017 I S. 2097ff.

[18] Kühling/Buchner, Datenschutz-Grundverordnung, DS-GVO Art. 17 Rn. 75.

[19] Stellungnahme Prof. Dr. Heinrich Amadeus Wolff zum DSAnpUG-EU vom 23.3.2017, S. 15.

[20] Siehe hierzu Schantz/Wolff, Das neue Datenschutzrecht, Rn. 1222 (mit Bezug auf Art. 23 Abs. 1 lit. i DS-GVO).

[21] Beispiel aus Kühling/Buchner, Datenschutz-Grundverordnung, DS-GVO Art. 30 Rn. 22.

[22] Art. 5 Abs. 2 sowie Art. 24 Abs. 1 DS-GVO.

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

UNTERSCHREITEN DES STANDS DER TECHNIK

Entscheidungsspielräume und Rechtsfolgen von Fehlentscheidungen nach Datenschutz-Grundverordnung und IT-Sicherheitsgesetz

Rechtsanwalt Karsten U. Bartels LL.M.

Neue nationale und gemeinschaftsrechtliche Gesetze sollen künftig das Niveau der IT-Sicherheit erhöhen. **Das zentrale Tatbestandsmerkmal für die IT-Sicherheit ist dabei wiederkehrend der Stand der Technik.** Der Stand der Technik findet sich nicht nur in der Datenschutz-Grundverordnung (DS-GVO), sondern ebenso im nationalen IT-Sicherheitsgesetz (ITSiG) sowie der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie).

Damit dieser objektiv-technische Begriff durch die Verpflichteten in der Praxis umgesetzt werden kann, enthalten die jeweiligen Normen zusätzlich, untereinander vergleichbare, subjektive Einschränkungen. Dies ermöglicht es Unternehmen (und je nach Anwendungsbereich der Norm auch Behörden), den **Stand der Technik rechtskonform zu unterschreiten.** Dabei geht es nicht um eine Umgehung eines gesetzlichen Niveaus oder die Vermeidung freiwilliger Investitionen in IT-Sicherheit. Vielmehr geht es um die notwendige Rechtssicherheit. Denn sämtliche IT-Sicherheitsmaßnahmen jederzeit nach dem Stand der Technik umzusetzen, erscheint praktisch unmöglich. Zum anderen muss den Gesetzesadressaten klar sein, welche Investitionen direkte Folge von gesetzlichen Verpflichtungen sind und welche nicht. Die subjektiven Kriterien werden maßgeblich für die Einhaltung von Verträgen und die Einstellung von aufsichtsbehördlichen Verfahren sein.

Objektives Tatbestandsmerkmal „Stand der Technik“

Die DS-GVO fordert von Unternehmen und Behörden, dass sie IT-Sicherheitsmaßnahmen auf dem Niveau des Stands der Technik einsetzen.

Zentrale Norm für die Sicherheit der Datenverarbeitung ist der Art. 32 DS-GVO.[1] Diese Norm sieht vor, dass Verantwortliche unter Berücksichtigung des Stands der Technik geeignete technische und organisatorische Maßnahmen zu treffen haben, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Auch das IT-Sicherheitsgesetz sieht Maßnahmen nach dem Stand der Technik für Betreiber *Kritischer Infrastrukturen* vor (§ 8a BSIG). KRITIS-Betreiber sind verpflichtet, zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT, angemessene organisatorische und technische Vorkehrungen zu treffen, bei deren Auswahl der Stand der Technik eingehalten werden soll.

Gleiches gilt durch die Umsetzung der NIS-Richtlinie gemäß § 8c BSIG für die Betreiber digitaler Dienste, bei denen es sich um Online-Marktplätze, Online-Suchmaschinen sowie Cloud-Computing-Dienste handelt. Betroffen sind Unternehmen, die mehr als 250 Personen beschäftigen und einen Jahresumsatz von über EUR 50 Mio. oder eine Jahresbilanz von über EUR 43 Mio. haben. Diese haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme zu bewältigen. Dabei haben sie ebenfalls den Stand der Technik zu berücksichtigen. Auch im Falle des § 13 Abs. 7 TMG, der sämtliche Unternehmen betrifft, die beispielsweise eine Website betreiben, ist der Stand der Technik im Rahmen der Sicherheit für Telemedienangebote zu berücksichtigen.

Die genannten Gesetze definieren den Stand der Technik allerdings nicht. Der Begriff beschreibt die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann. Es handelt sich damit um die am Markt verfügbaren Bestleistungen von Maßnahmen zum Schutz der IT-Sicherheitsziele. Daraus ergibt sich eine eindeutige Trennung zwischen dem objektiven Tatbestandsmerkmal des Stands der Technik und den Einschränkungen des objektiven Tatbestands durch subjektive Faktoren, die im Folgenden dargestellt werden.[2]

Subjektive Einschränkung des Stands der Technik

Das Tatbestandsmerkmal des Stands der Technik ist zunächst rein **objektiv zu ermitteln**. Allerdings beinhalten die gesetzlichen Regelungen **subjektive Einschränkungen**. Diese individuelle Begrenzung ist notwendig, um eine grundrechtskonforme Verhältnismäßigkeit herzustellen.

Bereits die Ermittlung des Stands der Technik erweist sich für viele Unternehmen als komplex. Die Implementierung der konkreten Maßnahmen ist aus technischen, organisatorischen, wirtschaftlichen sowie rechtlichen Gesichtspunkten häufig nicht zu leisten. Unternehmen müssen dann im Einzelfall beurteilen, welche Normen für sie gelten und welche Anforderungen diese an sie stellen. Subjektive Einschränkungsmöglichkeiten sind gesetzlich zumeist durch **technische und wirtschaftliche Faktoren** vorgegeben.

Die gesetzlichen Formulierungen zum Stand der Technik - wie „zu berücksichtigen“ oder „soll eingehalten werden“ - sind trotz unterschiedlicher Wortwahl rechtlich ähnlich und führen dazu, dass der Stand der Technik dem jeweiligen Kompromittierungsrisiko entsprechend in die Bewertung technischer und organisatorischer Maßnahmen einbezogen, aber nicht zwingend umgesetzt werden muss.[3]

Art. 32 DS-GVO und § 13 Abs. 7 TMG sehen weiterhin vor, dass bei der Umsetzung technischer Maßnahmen auch die **Implementierungskosten** ins Verhältnis gesetzt werden dürfen. Dies führt zu einer wirtschaftlichen **Verhältnismäßigkeitsprüfung**, im Rahmen derer das Verletzungsrisiko beachtet werden muss. Das Gesetz gibt zwar keine Anhaltspunkte für die zulässige Einbeziehung wirtschaftlicher Faktoren vor. Dies erweitert aber eher den Argumentationsspielraum, als ihn zu verengen.

Um den Nachweis der getroffenen Maßnahmen zu gewährleisten, als auch den Grad des Berücksichtigens darlegen zu können, ist eine entsprechende Dokumentation erforderlich. Dazu sollte

zunächst die Umsetzung des Tatbestandsmerkmals dokumentiert werden und in Bereichen, in denen der Technologiestand nicht erreicht wird, die eingesetzten Maßnahmen begründet werden. Dadurch kann eine **Berücksichtigung** belegt werden.

Rechtsfolgen der Unterschreitung des Stands der Technik

Eine Unterschreitung des Stands der Technik darf lediglich in rechtskonformer Weise erfolgen. Anderenfalls drohen **Bußgelder** und Ansprüche von Vertragspartnern.

Vertragliche Pflichten können zu erheblichen **Schadensersatzforderungen** führen, z. B. im Verhältnis Anbieter – Kunde oder Anbieter - Zulieferer. Dabei ist zu beachten, dass die IT-Sicherheit zum **Risikomanagement der Geschäftsleitung** gehört und aufgrund erheblicher Auswirkungen auf den Betrieb und auch dessen Reputation eine persönliche Haftung des Geschäftsführers oder Vorstandsmitglieds auslösen kann. ▸

[1] Bartels, Neue Anforderungen zum technischen Datenschutz nach der Datenschutz-Grundverordnung, BvD-News 1/2017, S. 22

[2] Bartels, Backer, Schramm; Der „Stand der Technik“ im IT-Sicherheitsrecht – Wirkung des Verweisungsbegriffs und Lösungsansätze zur legislativen Verwendung; in: Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, S. 503

[3] Bartels, Backer; „ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD – Datenschutz und Datensicherheit, 1/2016, 22-28, 27.

Fazit

Die Anforderungen an die gesetzliche IT-Sicherheit nach der DS-GVO sind hoch. Wer den Stand der Technik zu berücksichtigen hat, muss ihn objektiv-technisch ermitteln. Er darf allerdings subjektiv abwägen, ob und inwieweit er den Stand der Technik zulässig unterschreiten kann.

Eine Unterschreitung des Stands der Technik ist für den Normadressaten nur ratsam, wenn neben einer gewissenhaften Bewertung eingesetzter und einsetzbarer Maßnahmen eine umfangreiche Dokumentation erfolgt.

Eine rechtskonforme Unterschreitung kann dann aber zu erheblichen Einsparungen und organisatorischen Minderaufwänden führen. Es empfiehlt sich daher, im Rahmen der gesetzlich notwendigen Umsetzung der IT-Sicherheitsmaßnahmen technische und rechtliche Expertise einzuholen.

Das Risiko für eine Fehleinschätzung trägt der Verpflichtete. Die mögliche Unterschreitung des Stands der Technik sollte also jedenfalls mit der möglichen Übererfüllung abgewogen werden.

Über die Autoren

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

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

HK2 Rechtsanwälte

Datenschutz – Eine Vorschriftensammlung

4. Auflage 2017

Die Sammlung datenschutzrelevanter Gesetzesstellen wurde als Handwerkszeug für den betrieblichen Datenschutzbeauftragten konzipiert. Sie umfasst die wesentlichen Gesetzesvorschriften für den Umgang mit personenbezogenen Daten von Mitarbeitern, Kunden und Geschäftspartnern.

Hierzu liefert sie neben den grundsätzlichen Datenschutzvorschriften - Bundesdatenschutzgesetz (BDSG), EU-Datenschutzgrundverordnung (DS-GVO) und Bundesdatenschutzgesetz neue Fassung (BDSG n. F.) - die jeweils datenschutzrelevanten Abschnitte und Paragraphen aus über 60 Gesetzen und Verordnungen.

Die Europäische Datenschutzgrundverordnung DS-GVO und das Bundesdatenschutzgesetz neue Fassung (BDSG n. F.) werden am 25.05.2018 das heute gültige Bundesdatenschutzgesetz ablösen. Für das Verständnis und die Auslegung der DS-GVO spielen die 173 „Erwägungsgründe" eine wichtige Rolle, die ebenfalls in diese Textsammlung aufgenommen wurden. Als gute Orientierungshilfe dient zudem eine tabellarische Übersicht von Artikeln der DS-GVO und den Erwägungsgründen zu den entsprechenden Paragrafen des BDSG n.F."

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V (Hrsg.),
»Datenschutz – Eine Vorschriftensammlung«

4. Auflage 2017, 960 Seiten, A6, broschiert, Bestell-Nr. 60237, Ladenpreis 22,80 EUR (inkl. MwSt., zzgl. Versandkosten).

Die Vorschriftensammlung ist online bestellbar unter: www.tuev-media.de/bvd-dev.

BvD-Mitglieder finden im Mitgliederbereich unter

https://www.bvdnet.de/arbeitshilfen-fuer-bvd-mitglieder/

einen Bestellschein für die Bestellung als BvD-Mitglied.

Anzeige

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-Grundverordung
- Smart Home – Sicherung von Datenschutz und Privatsphäre

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

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

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

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

TÜVRheinland®
Genau. Richtig.

DATENSCHUTZ-ZERTIFIZIERUNG NACH DEM TRUSTED CLOUD DATENSCHUTZ-PROFIL FÜR CLOUD DIENSTE

Sascha Adler

Lokale Datenverarbeitungsanlagen werden immer häufiger durch Cloud-Dienste ersetzt. Deren Beliebtheit resultiert insbesondere aus der Skalierbarkeit und der Flexibilität, die Cloud-Dienste privaten und gewerblichen Nutzern zur Verfügung stellen können.

Inzwischen bieten nicht mehr nur große Konzerne Cloud-Dienste an; auch immer mehr kleine und mittlere Unternehmen halten Cloud Lösungen für spezielle Nutzeranforderungen bereit.

Werden auch personenbezogene Daten in der Cloud verarbeitet, müssen die Cloud-Nutzer sicherstellen, dass sämtliche datenschutzrechtlichen Vorgaben Beachtung finden. Zertifizierungen wie das Trusted Cloud Datenschutz-Profil für Cloud Dienste (kurz TCDP) können helfen, die gesetzlichen Pflichten zuverlässig zu erfüllen. Auch Cloud-Anbieter können dabei von einer Zertifizierung profitieren, die ihnen den Nachweis der Rechtskonformität ihres Dienstes gegenüber Jedermann ermöglicht.

Auftragsdatenverarbeitung ist Mittel der Wahl

Bei der Verarbeitung personenbezogener Daten Dritter sind grundsätzlich sowohl der Cloud-Nutzer als auch der Cloud-Anbieter verantwortliche Stelle. Für die Verarbeitung der personenbezogenen Daten des – ihm unbekannten – Dritten wird der Cloud-Anbieter in der Regel nicht über die erforderliche datenschutzrechtliche Rechtfertigung verfügen. Auch eine Einwilligung des Dritten hinsichtlich der Verarbeitungsmodalitäten, die beim Cloud-Anbieter bestehen, ist kaum praktikabel.

In aller Regel wird daher zwischen dem Cloud-Nutzer und dem Cloud-Anbieter eine Auftragsdatenverarbeitung gem. § 11 BDSG vereinbart. Der Cloud-Anbieter gilt dann nicht mehr als „Dritter" im Sinne von § 3 Abs. 8 S. 3 BDSG und die Verarbeitung wird so behandelt, als führe der Cloud-Nutzer sie unmittelbar selbst durch. Die Verantwortlichkeit für die Verarbeitung verbleibt so allein beim Cloud-Nutzer. Dafür muss der Nutzer nach den Vorgaben des § 11 Abs. 2 BDSG eine Vereinbarung über die Auftragsdatenverarbeitung mit dem Cloud-Anbieter abschließen, in der unter anderem auch die vom Anbieter zu treffenden technischen und organisatorischen Maßnahmen gem. § 9 BDSG festzulegen sind.

Da die Verantwortlichkeit für die Verarbeitung beim Cloud-Nutzer verbleibt, muss dieser sicherstellen, dass die Datenverarbeitung beim Cloud-Anbieter datenschutzkonform erfolgt und gem. § 11 Abs. 2 S. 4 BDSG regelmäßig die Einhaltung der vom Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen überprüfen. Hierzu werden insbesondere Privatpersonen oder kleine und mittlere Unternehmen im Regelfall nicht selbst in der Lage sein.

Zertifizierungen bieten Vorteile

Statt die erforderlichen Kontrollen selbst durchzuführen oder externe Dritte hiermit zu beauftragen, kann etwa auf unabhängige Zertifizierungen zurückgegriffen werden. Während eines Zertifizierungsprozesses überprüft ein unabhängiger Dritter anhand eines Kriterienkatalogs, ob die gesetzlichen Anforderungen an die gem. § 9 BDSG und der Anlage zu § 9 S. 1 BDSG notwendigen technischen und organisatorischen Maßnahmen eingehalten werden.

Ist dies der Fall, erwirbt der Cloud-Anbieter das Recht, seinen Dienst mit dem Zertifikat zu bewerben. Hierzu werden meist geschützte Siegel verwendet, die der Anbieter etwa auf seiner Internetpräsenz zeigt. Die Prüfung wird typischerweise zyklisch wiederholt, damit die Zertifizierung stets den aktuellen Gegebenheiten entspricht.

Für den Cloud-Anbieter ergeben sich verschiedene Vorteile: Er kann sich durch eine oder mehrere Zertifizierungen davor schützen, laufend durch eine Vielzahl von Cloud-Nutzern kontrolliert werden zu müssen. Gleichzeitig steht ihm eine werbewirksame Methode zur Verfügung, die Datenschutzkonformität seines Dienstes öffentlich zu dokumentieren.

Der Nutzer wird durch die Zertifikate in die Lage versetzt, einen Cloud-Dienst auszuwählen, bei dem die Einhaltung der technischen und organisatorischen Maßnahmen bereits von unabhängiger Seite festgestellt wurde und kann damit seiner Verantwortung zur Kontrolle des Anbieters ohne zusätzlichen Aufwand gerecht werden.

Der flexible Gesetzesmaßstab als Einschätzungsrisiko

Viele Zertifizierungen verfügen über einen einheitlichen, feststehenden Maßnahmenkatalog. Dies wird jedoch der gesetzlichen Verantwortung des Cloud-Nutzers nicht umfassend gerecht: § 9 BDSG sieht die Umsetzung derjenigen Maßnahmen vor, die erforderlich sind, um den Anforderungen des BDSG zu entsprechen. Als „erforderlich" werden in § 9 S. 2 BDSG solche Maßnahmen definiert, deren „Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht". Welche Arten von Maßnahmen hierbei in Betracht kommen, ergibt sich aus der Anlage zu § 9 S. 1 BDSG. Die Anlage nennt allerdings lediglich abstrakte Zielsetzungen, etwa die Verhinderung unberechtigten Zugriffs, die durch die konkret umzusetzenden Maßnahmen erfüllt werden müssen.

Jeder Cloud-Nutzer muss also bewerten, welche Maßnahmen für die jeweilige Datenverarbeitung erforderlich sind. Diese Bewertung kann von den Aufsichtsbehörden überprüft werden und ist von großer Tragweite: Weicht die Bewertung nach unten ab, waren die vorgesehenen Maßnahmen also nicht stark genug, um die gesetzlichen Anforderungen zu erfüllen, so stellt sich die Verarbeitung als rechtswidrig dar. Dies kann zu einem kompletten Verbot der Datenverarbeitung führen, womit im Extremfall ein Betriebsstillstand einhergeht. Sind die ergriffenen Maßnahmen dagegen stärker als erforderlich, sind zwar keine aufsichtsbehördlichen Sanktionen zu befürchten; die überobligatorischen Maßnahmen bieten aber auch keinen Mehrwert und schlagen gegebenenfalls finanziell zu Buche. ▸

DATENSCHUTZPRAXIS

Das Schutzklassenkonzept des TCDP

Um Cloud-Nutzern die Bewertung der erforderlichen Schutzmaßnahmen zu erleichtern, wurde im Rahmen des Pilotprojekts „Datenschutz-Zertifizierung für Cloud-Dienste“ des Bundesministeriums für Wirtschaft und Energie das Trusted Cloud Datenschutz-Profil für Cloud Dienste (TCDP) entwickelt.

Das TCDP sieht hierzu sog. „Schutzklassen“ vor. Das Schutzklassenkonzept ermöglicht es, die individuellen datenschutzrechtlichen Anforderungen an eine Verarbeitung zu bestimmen und anhand der ermittelten Anforderungen die Eignung des verwendeten Cloud-Dienstes zu prüfen. Hierzu unterscheidet das Schutzklassenkonzept zwischen Schutzbedarfsklassen und Schutzanforderungsklassen.

Anhand der Art der Daten und der Umstände der konkreten Datenverarbeitung kann der Cloud-Nutzer eine Schutzbedarfsklasse ermitteln, die seinen individuellen Anforderungen entspricht. Hierbei ist insbesondere die Sensitivität der zu verarbeitenden Daten von Bedeutung. Je einschneidender die Konsequenzen einer unbefugten Verarbeitung ausfallen würden, desto höher ist die Schutzbedarfsklasse zu wählen. Das TCDP sieht eine Einteilung in drei Schutzbedarfsklassen vor. Schutzbedarfsklasse 1 ist für personenbezogene Daten vorgesehen, bei denen auch bei unbefugter Verarbeitung meist nicht mit einem konkreten Nachteil zu rechnen ist, etwa Name und Anschrift einer Person. Schutzbedarfsklasse 3 entspricht dagegen einem hohen Schutzbedarf für Daten, bei deren unbefugter Verarbeitung es zu schwerwiegenden Nachteilen für den Betroffenen kommen kann. Beispiele hierfür sind etwa Patientendaten oder Informationen zu strafrechtlichen Verurteilungen. Die Einschätzung, welche Schutzbedarfsklasse angemessenen Schutz bietet, obliegt dabei dem Nutzer.

Spiegelbildlich zu den Schutzbedarfsklassen werden auf der Seite des Cloud-Anbieters drei Schutzanforderungsklassen definiert. Jeder Cloud-Anbieter ordnet seinen Dienst einer Schutzanforderungsklasse zu. Im Rahmen der Zertifizierung wird dann geprüft und dokumentiert, ob der Dienst den Anforderungen der gewählten Schutzanforderungsklasse gerecht wird. Höhere Klassen beinhalten dabei höhere Anforderungen an die umzusetzenden technischen und organisatorischen Maßnahmen.

Der Cloud-Nutzer ist somit in der Lage, anhand der von ihm vorgenommenen Ermittlung des Schutzbedarfs einen Cloud-Dienst der korrespondierenden Schutzanforderungsklasse zu wählen und damit sicherzustellen, dass seine Daten unter angemessenen Bedingungen verarbeitet werden. Gleichzeitig ist es nicht erforderlich, dass der Nutzer sämtliche technischen und organisatorischen Maßnahmen, die der Anbieter ergreift, daraufhin überprüft, ob diese seinem Schutzbedarf entsprechen.

Standardisierung des Vertrages zur Auftragsdatenverarbeitung

Da das TCDP unter Beteiligung von Industrie, Aufsichtsbehörden, Prüfstellen und Rechtsexperten entwickelt und vom Bundesministerium für Wirtschaft und Energie gefördert wurde, konnten die Anforderungen aller Beteiligten an eine Zertifizierung für Cloud-Dienste umfassend berücksichtigt werden. Das TCDP enthält so neben der konkreten Regelung der technischen und organisatorischen Maßnahmen auch viele weitere Regelungselemente und geht damit über den Umfang rein technischer Zertifizierungen hinaus.

Detailliert geregelt sind insbesondere die Anforderungen an den gem. § 11 BDSG abzuschließenden Vertrag über die Auftragsdatenverarbeitung. Die vertraglichen Regelungen zwischen Cloud-Nutzer und Anbieter werden im Rahmen der TCDP-Zertifizierung daraufhin überprüft, ob sie dazu geeignet sind, die gesetzlichen Rechte und Pflichten der Parteien angemessen abzubilden. Hierzu zählen insbesondere die notwendigen Regelungen zur Weisungsgebundenheit des Cloud-Anbieters sowie die hiermit in Verbindung stehenden Informations- und Mitteilungspflichten.

Schließt der Nutzer mit einem TCDP-zertifizierten Cloud-Anbieter einen Vertrag über die Auftragsdatenverarbeitung ab, so kann er sich darauf verlassen, dass der Vertrag es ihm ermöglicht, seine gesetzlichen Verpflichtungen angemessen zu erfüllen.

Vorteil modulare Zertifizierung

Ein weiterer Vorteil des TCDP besteht in dessen modularer Konzeption. Die Prüfung und Zertifizierung eines Cloud-Dienstes kann erheblichen Aufwand und damit auch hohe Kosten verursachen. Zugleich sind einzelne Elemente eines Cloud-Dienstes häufig stark miteinander verzahnt und einzelne Komponenten stetigen Veränderungen unterworfen, etwa wenn neue Funktionalitäten implementiert werden. Bei solchen Änderungen ist dann häufig eine erneute Bewertung erforderlich, ob die Vorgaben der Zertifizierung weiterhin erfüllt werden.

Das TCDP ermöglicht es, einzelne Module des Cloud-Dienstes getrennt voneinander zu zertifizieren. Daher muss bei Veränderung einzelner Bestandteile nicht zwingend der gesamte Dienst neu bewertet werden. Stattdessen können die veränderten Bestandteile und deren Zusammenspiel mit den übrigen Modulen jeweils gesondert betrachtet werden. Dies spart bei Veränderungen in erheblichem Maße Kosten, was insbesondere für kleine und mittlere Unternehmen, die Cloud-Dienste anbieten, einen bedeutenden Vorteil darstellt.

Die Weiterentwicklung des TCDP im Rahmen der Datenschutz-Grundverordnung

Das TCDP stellt derzeit neben ISO-Normen vor allem auf die Anforderungen des geltenden BDSG ab, welches im kommenden Frühjahr abgelöst wird. Ein Projekt zur Entwicklung einer Nachfolgezertifizierung auf Grundlage der datenschutzrechtlichen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) und des sie begleitenden neuen BDSG ist aber bereits initiiert worden. Ziel dieses Projektes ist es, auch für die Zeit ab Geltung der DS-GVO eine Zertifizierungslösung auf Grundlage des TCDP zu schaffen, wobei auch eine Überleitung bestehender Zertifizierungen auf die neue Rechtsgrundlage ermöglicht werden soll.

Die Rahmenbedingungen der DS-GVO für Zertifizierungslösungen zur Datenschutzkonformität sind wesentlich strenger als die des BDSG. Art. 42 DS-GVO sieht explizit die Einführung von Zertifizierungsprogrammen vor, wobei unter anderem auch die Einhaltung der Vorgaben der DS-GVO für Auftragsverarbeiter – die den bisherigen Auftragsdatenverarbeitern des BDSG funktional entsprechen – adressiert wird.

Hinsichtlich der erforderlichen technischen und organisatorischen Maßnahmen werden die Anforderungen der DS-GVO voraussichtlich mit denen des BDSG vergleichbar bleiben. Auftragsverarbeiter sind gem. Art. 28 Abs. 1 DS-GVO weiterhin zur Umsetzung der notwendigen technischen und organisatorischen Maßnahmen verpflichtet. Welche Maßnahmen erforderlich sind, ist gegenüber der Anlage zu § 9 S. 1 BDSG zwar wesentlich unbestimmter, insbesondere Art. 32 DS-GVO und Erwägungsgrund 39 sehen aber ebenfalls etwa Maßnahmen zur Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie Zugangs- und Zugriffsbeschränkungen vor. Zudem legt Art. 24 Abs. 1 DS-GVO hinsichtlich der Verhältnismäßigkeit fest, dass bei den Sicherheitsmaßnahmen eine unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken zu berücksichtigen ist.

Dadurch, dass Zertifizierungsverfahren künftig deutlich stärker reglementiert werden und diese gem. Art. 42, 43 DS-GVO nur unter Mitwirkung der zuständigen Aufsichtsbehörde und der staatlichen Akkreditierungsstelle entwickelt und vergeben werden dürfen, wird sich der Markt für entsprechende Zertifizierungen voraussichtlich stark verändern. Innerhalb des von der Stiftung Datenschutz begleiteten Nachfolgeprojekts zum TCDP werden bereits in der Entwicklungsphase sowohl Aufsichtsbehörden als auch die Deutsche Akkreditierungsstelle beteiligt. Hierdurch wird sichergestellt, dass die Nachfolgezertifizierung frühestmöglich DS-GVO-konform eingesetzt werden kann.

Über den Autor

Ass. iur. Sascha Adler

unterstützt die Stiftung Datenschutz bei sämtlichen Fragen zum Trusted Cloud Datenschutz-Profil TCDP. Er ist Doktorand bei Prof. Dr. Georg Borges.

STIFTUNG DATENSCHUTZ

DATENSCHUTZPRAXIS – ADVERTORIAL

DS-GVO LEGT FOKUS AUF DATENSICHERHEIT

Christian Volkmer

Die technischen und organisatorischen Maßnahmen müssen stets dem „Stand der Technik" entsprechen

Die neue EU-Datenschutzgrundverordnung fordert neben Datenschutz auch die Datensicherheit ein. „Sie verlangt in Artikel 32 eine durchaus komplexe Abwägung zwischen dem möglichen Risiko, dem Stand der Technik und den Kosten zu treffen", erläutert Christian Volkmer, geschäftsführender Inhaber des Regensburger Datenschutzanbieters Projekt 29. Daran haben sich „geeignete" technische und organisatorische Maßnahmen (TOM) zu orientieren (siehe Kasten: Art. 32 DS-GVO).

Christian Volkmer, Projekt 29 GmbH & Co. KG

Volkmer bleibt zunächst in der analogen Welt, um das Begriffspaar technische und organisatorische Maßnahmen zu erläutern. Zum Schutz von Personalakten könnte die technische Maßnahme sein, sie in einem verschlossenen Stahlschrank aufzubewahren. Dazu gehört als organisatorische Maßnahme eine Richtlinie, wie der Schlüssel zum Schrank verwahrt wird und wer Zugang zum Schlüssel bekommt.

„Übertragen in die digitale Welt stellen sich hier nach DS-GVO sofort einige Fragen", so der Experte. Zunächst gilt es, das Risiko zu bestimmen. Wie schutzbedürftig sind die Daten? Hier muss für die eigene Organisation der Schutzbedarf personenbezogener Daten zum Beispiel nach „normal", „hoch" und „sehr hoch" eingestuft werden. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat den Standard 100-2 eingeführt, der den Schutzbedarf nach den oben genannten Stufen definiert.

Im Zuge einer Risiko-Folgenabschätzung muss in die Abwägung einfließen, was schlimmstenfalls passieren könnte, wenn die Daten verloren gehen oder unbefugt in die Hände Dritter gelangen. „Kann der Datendieb lediglich unerwünschte Werbemails verschicken, liegt die Sache sicher anders, als wenn er Zugang zum Bankkonto des Betroffenen erhält", erläutert Volkmer.

Was gilt als „Stand der Technik"?

Welche Maßnahmen sind also „geeignet" das Risiko abzuwenden? Und zwar unter Berücksichtigung des „Stands der Technik" und der „Implementierungskosten"?

„‚Stand der Technik' ist juristisch eine Generalklausel. Was sie konkret meint, ist nirgendwo wirklich festgelegt, alleine schon, weil sich die Technik in der EDV ja rasant weiterentwickelt", sagt Volkmer. „Stand der Technik" liegt dabei zwischen den „allgemein anerkannten Regeln der Technik" und dem „Stand der Wissenschaft und Technik". Die Abgrenzung dieser drei Generalklauseln fließt und verändert sich ständig. Deswegen muss jede Organisation für die korrekte Einstufung nach DS-GVO den „Stand der Technik" bezogen auf ihre Systeme regelmäßig neu bewerten. Ziel ist, die technischen und organisatorischen Maßnahmen nachvollziehbar zu dokumentieren, sodass die Datenschutz-Aufsichtsbehörde sie im Fall der Fälle fundiert und notfalls gerichtsfest überprüfen kann.

Die Generalklausel „Stand der Technik" meint das obere Ende des technisch Möglichen und praktisch Bewährten. „Die auf einen Stichtag bezogene Abgrenzung zwischen dem ‚Stand der Technik' und den ‚anerkannten Regeln der Technik' kann durchaus knifflig sein", sagt Christian Volkmer. Deswegen kann es sich bei besonders hohem Risiko sogar empfehlen, einen externen Sachverständigen die TOM überprüfen zu lassen.

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat eine Hilfestellung angekündigt. Die Beamten wollen einen Fragebogen zur Verfügung stellen, der abzuschätzen hilft, ob die eigenen TOM dem Stand der Technik entsprechen.

Für die Datensicherheit greift ein Prinzip, das die DS-GVO insgesamt in den Datenschutz einführt. „Ohne Managementsysteme nach ▸

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-Richtlinie ist das Datenschutzrecht im Umbruch. Erst nach und nach kristallisieren sich die Vorstellungen der Aufsichtsbehörden zur korrekten Umsetzung der Paragrafen 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 Onlinelösung, 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 DPROREG, 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

dem PDCA-Zyklus wird es nicht mehr gehen“, ist Volkmer überzeugt. Erst der ständige Prozess aus Planung (P wie Plan), der Umsetzung im Unternehmensalltag (D wie Do), der regelmäßigen Evaluierung (C wie Check) – bei TOM der Bemessung am Stand der Technik – und letztlich der Verbesserung (A wie Act) führt zu einer Umsetzung im Sinne des neuen europäischen Datenschutzrechts. „Nachdem jetzt sowieso alle gefordert sind, ihre Datenschutzpraxis neu zu justieren, lohnt sich die Überlegung, auch gleich ein Informationssicherheits-Management einzuführen“, regt der Experte an.

Spezialsoftware mit Technik-Check

„Unternehmen, Verbände, Freiberufler und deren Datenschutzbeauftragte brauchen Werkzeuge, die ihnen Arbeit abnehmen“, sagt Volkmer. Darin hat Projekt 29 langjährig Erfahrung. Volkmer und seine Mitarbeiter halten aktuell bundesweit über 2.500 Mandate als externe Datenschutzbeauftrage 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.

Auch das Thema Datensicherheit bildet Privacysoft ab. Basierend auf Experten-Informationen und Hilfestellungen wie dem Fragebogen des BayLDA stellt die Software Checklisten zur Verfügung. Mit automatischer Terminierung, zum Beispiel einmal jährlich, hilft das System beim fälligen Technik-Audit.

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

Art 32 DS-GVO (Auszug)

„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 des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; …“

Anzeige

Mit Privacysoft entspannt zurücklehnen

Das Allround-Werkzeug für alle Datenschutzaufgaben

© shutterstock.com – dotshock

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 revisionssichere 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 Demotermin-Vereinbarung 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.

Ostengasse 14, 93047 Regensburg, Tel. 0941 2986930
www.privacysoft.de

Projekt 29

DATENSCHUTZPRAXIS

DIENSTLEISTER IM GESUNDHEITSWESEN

Barbara Stöferle – Sprecherin des AK Medizin des BvD

Eine moderne Gesundheitsversorgung ist ohne den Einsatz von Dienstleistern nicht denkbar, sei es für die Übernahme von spezialisierten Aufgaben, sei es zur Einsparung von Kosten.

Dienstleistungen wie beispielsweise Wartung von medizinischen Geräten, IT-Support, Arztbriefschreibung, Archivierung fallen aus Sicht des Datenschutzes i.d.R. unter den Begriff der Auftragsdatenverarbeitung. Diese wird nun in der Datenschutz-Grundverordnung neu geregelt. Daher haben die vier Verbände BvD, bvitg, GDD und GMDS zusammen mit der DKG ihren Muster-AV-Vertrag für das Gesundheitswesen an die neue Situation angepasst und zusätzlich Hinweise zum Umgang mit Altverträgen erarbeitet.

Zusätzlich zur neuen DS-GVO haben sich auch Neuerungen beim § 203 StGB ergeben, die Auswirkungen auf den zulässigen Einsatz von Dienstleistern haben werden.

Auftragsverarbeitung unter der DS-GVO

BDSG, LDSG und SGB X kennen bisher schon den Begriff einer Auftragsdatenverarbeitung (ADV).

Bindet man einen Dienstleister, also einen Dritten im Sinne der bisherigen Datenschutzgesetze, vertraglich entsprechend §11 BDSG oder § 80 SGB X bzw. vergleichbaren LDSG- bzw. kirchlichen Datenschutz-Regelungen als Auftragsdatenverarbeiter eng ein, so ist dieser Dienstleister nicht mehr ein Dritter im Sinne des Gesetzes. Der Dienstleister ist sozusagen „verlängerter Arm“ der verantwortlichen Stelle und handelt ausschließlich weisungsabhängig. Der Auftraggeber behält volle Verfügungsgewalt über die Daten und auch die Verantwortung über deren Verarbeitung. Es werden zwar Daten an den Dienstleister übergeben. Dies stellt aber aus Sicht des Datenschutzes keine Datenübermittlung dar. Damit wird keine gesetzliche Legitimation oder Einwilligung über die Übergabe der Daten zur Ausübung der Dienstleistung benötigt. Eine Auftragsdatenverarbeitung gilt an dieser Stelle als privilegiert.

Ab dem 25. Mai 2018 gilt die EU Datenschutz-Grundverordnung (DS-GVO). Auch hier findet sich in Art. 28 DS-GVO eine entsprechende Regelung zur Auftragsverarbeitung, die ähnlich der ADV eine Auftragsverarbeitung (AV) privilegiert. Die bisherigen Regelungen im BDSG, LDSG, SGB X oder den kirchlichen Datenschutzgesetzen entfallen bzw. müssen vom jeweiligen Gesetzgeber an die Anforderungen des Art. 28 DS-GVO angepasst werden.

Bis zum 25. Mai 2018 müssen nun alle bestehenden Verträge zur Auftragsdatenverarbeitung (ADV) geprüft werden, ob sie den neuen Anforderungen zur Auftragsverarbeitung (AV) genügen. Ebenso ist zu betrachten, ob sich bezüglich anderer Verträge mit Dienstleistern Änderungen ergeben werden.

Änderungen bei AV

Auf den ersten Blick mag der Art. 28 DS-GVO im Vergleich zum „alten“ § 11 BDSG ähnlich aussehen. Aber genauer betrachtet ergeben sich durchaus Änderungen, die zwingend beachtet und umgesetzt werden müssen.

Grundsätzlich gleich geblieben sind die Merkmale, die für eine AV sprechen:

- Weisungsabhängige Tätigkeit
- Verantwortlicher behält Zugriff auf die Daten bzw. deren Verarbeitung
- Verantwortlicher bleibt für die Rechtsgrundlage der Verarbeitung verantwortlich und behält die Pflichten für die Verarbeitung
- Auftragsverarbeiter führt eine Hilfsfunktion mit nur geringem Handlungs-, Gestaltungs- oder Entscheidungsspielraum aus
- Auftragsverarbeiter hat ein Nutzungsverbot außerhalb des Auftrags

Wie bisher müssen zwischen Verantwortlichem (Auftraggeber) und Auftragsverarbeiter (Auftragnehmer, Dienstleister) vertraglich geregelt werden:

- Gegenstand und Dauer des Auftrags
- Umfang, Art und Zweck der Verarbeitung
- Art der Daten
- Kategorien betroffener Personen
- Umgang und Gewährleistung der Betroffenenrechte
- Pflichten und Rechte des Verantwortlichem
- Art und Umfang der Weisungsbefugnisse des Verantwortlichen gegenüber dem Auftragsverarbeiter
- Pflichten des Auftragsverarbeiters
- Kontrollrechte des Verantwortlichen sowie zugehöriger Pflicht zur Unterstützung durch den Auftragsverarbeiter
- Berechtigung zum Einschalten von Unterauftragsverhältnissen
- Umgang mit mitteilungspflichtigen Verstößen oder Verstößen gegen vertragliche Regelungen
- Rückgabe bzw. Löschen der Daten bei Auftragsende

Manche dieser Punkte sind verändert bzw. spezifiziert worden.

Auf den ersten Blick fallen die neuen Begrifflichkeiten wie „Verantwortlicher“ statt „Auftraggeber“ oder „Auftragsverarbeiter“ statt „Auftragnehmer“ auf, die aber von der Bedeutung nahezu unverändert geblieben sind.

Die Bedeutung des Begriffs der „Verarbeitung“ hat sich für die Einordnung von Tätigkeiten, die unter Auftragsverarbeitung fallen, geändert.

Unter dem BDSG musste sich die ausgelagerte Tätigkeit auf die Datenverarbeitung oder eine Phase der Datenverarbeitung (z.B. Erheben oder Löschen) beziehen. Weisungsabhängige Tätigkeiten, bei denen die Daten als „Beiwerk“ zur eigentlichen Tätigkeit dem Dienstleister zur Verfügung gestellt werden, fielen nach Auffassung mehrerer Aufsichtsbehörden[1] und in der überwiegenden Meinung der Fachliteratur nicht unter ADV. Typische Beispiel im Krankenhaus hierzu war die Speisenversorgung, bei der der Kern der Tätigkeit die Essensversorgung der Patienten im Mittelpunkt des Auftrags stand und hierzu eben als Beiwerk Daten zur korrekten Essensversorgung benötigt werden.

Unter der DS-GVO ist der Begriff der Verarbeitung, auf den sich auch der Art. 28 DS-GVO bezieht, neu zu interpretieren. In Art. 4 Abs. 1 Nr. 2 DS-GVO wird „Verarbeitung“ ausdrücklich technikneutral formuliert. Dies wird auch im zugehörigen Erwägungsgrund 15 ausgeführt. Im Kurzpapier Nr. 5 der DSK zum Thema Datenschutz-Folgenabschätzung steht zum Begriff Verarbeitung: „Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen.“[2] Hieraus folgend hat die Arbeitsgruppe den Begriff der Verarbeitung folgendermaßen erläutert[3]:

> *„Der Begriff der Verarbeitung aus der DS-GVO beschränkt im Gegensatz zum BDSG eine Auftragsverarbeitung nicht auf eine rein technische Unterstützung.“*

Dies bedeutet, dass bei der Einordnung von ausgelagerten Tätigkeiten in AV oder Funktionsübertragung nicht nur die Daten bzw. das IT-System zu betrachten sind, sondern der komplette Prozess. Daraus folgt, dass wesentlich mehr weisungsabhängige Beauftragungen künftig unter die Regelungen einer Auftragsverarbeitung ▸

[1] https://www.lda.bayern.de/media/info_adv.pdf

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/03/H_AuftragsDV_Funktionsuebertragung.pdf

https://www.lfd.niedersachsen.de/themen/auftragsdatenverarbeitung/auftragsdatenverarbeitung_im_nichtoeffentlichen_bereich_11_bdsg/datenschutzgerechte-auftragsdatenverarbeitung-139458.html

[2] http://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html

[3] https://www.bvdnet.de/wp-content/uploads/2017/07/17_Umgang_Altvertraege.pdf

DATENSCHUTZPRAXIS

fallen werden. In der Praxis wird dies eher eine Erleichterung als zusätzliche Anforderungen bringen. Zukünftig können alle solchen Dienstleistungen als Auftragsverarbeitung entsprechend den Vorgaben der DS-GVO gestaltet werden, ohne dass Überlegungen zur Zulässigkeit einer Datenübermittlung angestellt werden müssen, da diese unter der Begrifflichkeit „Verarbeitung" subsumiert sind und somit als AV im Sinne von Art. 28 DS-GVO zulässig sein können. Ein Vertrag mit dem Dienstleister, der ähnlich einem ADV-Vertrag aufgebaut und in dem der Umgang Daten des Patienten geregelt waren, war bisher schon dringend empfehlenswert; zukünftig wird für ein solches Szenario eindeutig ein AV-Vertrag abgeschlossen. Weiterhin muss bedacht werden, dass ohne Auftragsverarbeitung und entsprechenden Vertrag ein Dienstleister einen eigenen rechtlichen Erlaubnistatbestand zur Verarbeitung der Daten benötigen würde, da er dann ja Dritter im Sinne der DS-GVO wäre und der rechtliche Erlaubnistatbestand des Verantwortlichen i.d.R. die Weitergabe von Daten an Dritten nicht abdeckt.

Exemplarisch für geänderte vertragliche Regelungen bei AV unter der DS-GVO seien die Punkte Unterauftragnehmer, technisch-organisatorische Maßnahmen und Vertraulichkeitsverpflichtung herausgegriffen:

Bei Unterauftragnehmern verlangte die bisherige Regelung im BDSG lediglich eine Festlegung hinsichtlich der Berechtigung zur Begründung von Unterauftragsverhältnissen. Unter der DS-GVO dürfen Unterauftragnehmer nur nach schriftlicher Genehmigung durch den Auftraggeber eingeschaltet werden. Auch bei einer allgemeinen Genehmigung zur Einschaltung von Unterauftragnehmers muss der Auftraggeber bei Änderungen informiert werden. So soll sichergestellt werden, dass der Auftraggeber als Verantwortlicher stets informiert ist, durch wen und wie seine Verarbeitung durchgeführt wird.

Die geeigneten technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO müssen auch weiterhin gemeinsam festgelegt werden. Dabei fallen sowohl der Verantwortliche als auch der Auftragsverarbeiter unter die Regelung, d.h. im Gegensatz zum BDSG bekommt der Auftragsverarbeiter eigene Pflichten auferlegt. Zudem fallen die relativ starren Vorgaben, aufgelistet nach Maßnahmen, aus der Anlage zu § 9 S. 1 BDSG weg. Vielmehr steht zukünftig ein risikobasierter Ansatz der zu treffenden Maßnahmen inklusive entsprechender Dokumentations- und Nachweispflichten im Vordergrund.

Der Auftragsverarbeiter muss gemäß Art. 28 Abs. 3 S. 2 lit. c DS-GVO gewährleisten, dass alle mit der Verarbeitung betrauten Personen zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

Neu hinzugekommen unter der DS-GVO sind:

- Die räumliche Beschränkung der Auftragsverarbeitung, wie sie in § 3 Abs. 8 S. 3 BDSG enthalten ist, fällt weg. Sind die entsprechenden Verhältnisse gegeben, kann eine Auftragsverarbeitung künftig weltweit erfolgen.
- Regelungen zu Vertretungsregelung des Auftragsverarbeiters, wenn ein Drittstaatenbezug gemäß Art. 3 Abs. 2 vorliegt (Art. 27 DS-GVO).
- Die Beschränkungen für den Datentransfer in Drittländer (z.B. im Rahmen von Software-Pflege) sind auch vom Auftragsverarbeiter zu beachten (Art. 44 DS-GVO)
- Möglichkeit, angemessene technisch-organisatorische Maßnahmen durch Einhaltung genehmigter Verhaltensregeln (Art. 40 DS-GVO) oder eines genehmigten Zertifizierungsverfahrens (Art. 42 DS-GVO) nachzuweisen
- Dokumentation und Nachweispflichten der Verarbeitungen durch den Auftragsverarbeiter
- Bußgeldregelungen sind allgemein unter der DS-GVO erweitert und betreffen Verantwortlichen und Auftragsverarbeiter
- Haftung des Auftragsverarbeiters
- Schadensersatzansprüche der betroffenen Personen sowohl gegen Verantwortlichen als auch Auftragsverarbeiter möglich
- Führung eines Verzeichnisses von Verarbeitungstätigkeiten beim Auftragsverarbeiter
- Die Pflicht zur Bestellung eines Datenschutzbeauftragten kann auch für den Auftragsverarbeiter gelten (Art. 37 DS-GVO)

Muster-AV-Vertrag für das Gesundheitswesen

Neben diesen Vorgaben bei der Beauftragung von Dienstleistern kommen im Gesundheitswesen zusätzliche Anforderungen bei der Gestaltung eines AV-Vertrags hinzu.

Manche Abwägungen (wie z. B: angemessene Maßnahmen bei der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO bemessen sich am Schutzbedarf und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Personen. Dies ist bei Gesundheitsdaten wesentlich höher einzuschätzen als beispielsweise bei ebenfalls schützenswerten Gehaltsdaten oder Kundendaten.

Darüber hinaus gibt es weitere Besonderheiten wie beispielsweise

- Sozialdaten,
- Umgang mit §203 StGB sowie dem Beschlagnahmeschutz,
- Regelung bzgl. Umgang mit Zurückbehaltungsrecht i.S.v. § 273 BGB,
- Schadensersatz- und Haftungsfragen,
- Umgang mit Zweckänderung durch den Auftragnehmer, z.B. Weitergabe der Daten nach Pseudonymisierung/Anonymisierung,
- … (die Liste könnte noch fortgeführt werden).

Betrachtet man die Einsatzszenarien für eine Auftragsverarbeitung, so hat ein Krankenhaus sehr viele Verträge mit unterschiedlichsten Dienstleistern, angefangen bei Arztbriefschreibung, IT-Support, Patiententransport zu Untersuchungen, Software-Wartung für viele Spezialanwendungen, Speisenversorgung, Reinigungsdienstleistung bis hin zu Wartungsverträge für Medizingeräte (MRT, CT, Röntgengerät, Endoskop, Infusionsgeräten) vieler Hersteller.

Daher hat sich im Jahr 2014 eine Arbeitsgruppe bestehend aus Vertretern von

- Berufsverband der Datenschutzbeauftragten Deutschlands e. V., BvD (Arbeitskreis „Medizin")
- Bundesverband Gesundheits-IT e. V., bvitg
- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V., GMDS (Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen")
- Gesellschaft für Datenschutz und Datensicherheit e. V., GDD (Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen")

zusammengesetzt, um einen Muster-ADV-Vertrag für die besonderen Anforderungen im Gesundheitswesen miteinander abzustimmen.

Hier sind nicht nur die Besonderheiten im Gesundheitswesen abgedeckt, sondern dieses Muster sollte auch eine Orientierung zur Vereinheitlichung bei der Vielzahl von Verträgen geben.

Für die Anpassung dieses Muster-Vertrages an die DS-GVO konnte die Deutsche Krankenhausgesellschaft (DKG) mit in die Arbeitsgruppe geholt werden.

So entstand ein an die DS-GVO angepasster Muster-AV-Vertrag, der die Besonderheiten im Gesundheitswesen abdeckt. Verbände aller Akteure bei Beauftragungen im Gesundheitswesen haben eine gemeinsame AV-Vertragsvorlage gestaltet, die umfangreiche Kommentierungen beinhaltet. Durch alternative und optionale Formulierungen sind die Interessen sowohl von Krankenhäusern als Verantwortliche als auch Dienstleistern oder IT-Herstellern als Auftragsverarbeiter vertreten. Der Muster-AV-Vertrag eignet sich daher für viele Einsatzgebiete einer AV im Gesundheitswesen auch außerhalb von Krankenhäusern wie z.B. Arztpraxen, Medizinischen Versorgungszentren, sozialen Einrichtungen, etc. Da der Vertrag unter einer Creative Commons-Lizenz veröffentlicht wurde, darf er unter den genannten Lizenzbedingungen an die eigenen Gegebenheiten angepasst und verwendet werden.

Um die Umstellung auf die DS-GVO bei Altverträgen zu erleichtern, gibt es zusätzlich eine Ausarbeitung, die detailliert auf beibehaltene, geänderte und neue Regelungen zur Auftragsverarbeitung unter der DS-GVO eingeht.

▸

DATENSCHUTZPRAXIS

Der Muster-AV-Vertrag ist auf den Webseiten der beteiligten Verbände zu finden:

BvD:

https://www.bvdnet.de/bvd-arbeitskreise/arbeitskreis-medizin/

bvitg:

http://www.bvitg.de

GMDS:

http://ds-gvo.gesundheitsdatenschutz.org/html/adv-vertrag.php

DKG:

http://www.dkgev.de/dkg.php/cat/130/title/Datenschutz___aerztliche_Schweigepflicht

GDD:

https://www.gdd.de/arbeitskreise/datenschutz-und-datensicherheit-im-gesundheits-und-sozialwesen/materialien-und-links

Schweigepflicht und Auftragsverarbeitung

Getrennt zu den datenschutzrechtlichen Voraussetzungen sind bei einer AV zusätzlich die Anforderungen des Strafrechts zu beachten. Sowohl das BDSG (§1 Abs. 2 S. 2) als auch die DS-GVO (Art. 9 Abs. 3 DS-GVO) schließen sich als Befugnisnorm zur Offenbarung von Privatgeheimnissen aus.

Da bei einer Beauftragung von Dienstleistern oftmals Patientendaten offenbart werden (müssen) bzw. die Offenbarung nicht ausgeschlossen werden kann, ist eine spezialgesetzliche Offenbarungsbefugnis im Sinne des §203 StGB (Verletzung von Privatgeheimnissen, „ärztliche Schweigepflicht“) erforderlich. (Auf die theoretische Möglichkeit, ein Einverständnis des Patienten einzuholen, wird hier nicht eingegangen, da dies im Alltag weder praktikabel ist noch immer eine Freiwilligkeit gegeben ist.)

Die Gesetzeslandschaft bei Zulässigkeit einer Auftrags(daten)verarbeitung ist sehr unterschiedlich. In vielen Landeskrankenhausgesetzen finden sich Erlaubnistatbestände für die AV, die von „im Krankenhaus selbst“ über „Vermeidung von Störungen im Betriebsablauf“ bis hin zu „erlaubt bei Einhaltung der datenschutzrechtlichen Bestimmungen“ gehen. Außerhalb des Krankenhausbereiches bzw. in Bundesländern ohne entsprechendes Krankenhausgesetz gab es bisher keine Erlaubnistatbestände für die Offenbarung von Patientendaten im Rahmen einer Auftrags-(daten)verarbeitung.

Der Gesetzgeber und Aufsichtsbehörden wurden immer wieder darauf hingewiesen, dass sich ein Arzt persönlich in die Gefahr begibt, einen Schweigepflichtsverstoß zu begehen, wenn er beispielsweise für seine Arztpraxis einen professionellen Dienstleister für die fachgerechte Betreuung der IT-Systeme beauftragt. Immerhin könnte der Mitarbeiter des Dienstleisters mit den für die Tätigkeit erforderlichen Administratorrechten evtl. in die elektronische Patientenakte Einsicht nehmen. Dass eine professionelle IT-Betreuung in einer Arztpraxis sinnvoll ist, steht außer Frage. Oftmals wurden solche Personen als „Gehilfen“ des Arztes angesehen, was aber vor allem bei externen Personal in Fachkreisen äußerst umstritten war. Dies führte im Alltag zu unverständlichen Situationen, dass beispielsweise eine externe Arztbriefschreibung datenschutzrechtlich nach Abschluss eines Vertrags absolut rechtskonform war, bezüglich der Schweigepflicht in einem Krankenhaus in Hamburg zulässig, in bayrischen oder baden-württembergischen Krankenhaus aber eine Entbindung von der Schweigepflicht durch den Patienten notwendig war, weil in diesen Bundesländern keine gesetzliche Offenbarungsbefugnis vorhanden war.

Endlich hat der Gesetzgeber diese Lücke geschlossen, in dem der Personenkreis, der dem §203 StGB unterliegt bzw. eine Offenbarung zulässig ist, erweitert worden ist. Bisher fielen u.a. der Berufsgeheimnisträger selbst, die berufsmäßig tätigen Gehilfen (z.B. medizinische Fachangestellte, Radiologieassistenten) und die zur Vorbereitung auf den Beruf tätigen Personen unter die berufliche Schweigepflicht. Die Weitergabe von Informationen an diese Personengruppen durch die Berufsgeheimnisträger ist von vornherein kein Bruch der Schweigepflicht.

Neu hinzugekommen sind die „sonstige mitwirkende Personen“. Gegenüber diesem Personenkreis ist die Offenbarung befugt, sofern eine solche für die Tätigkeit der sonstigen mitwirkenden Person erforderlich ist. Damit ist die Diskussion, ob Berufsgruppen wie ITler, Patiententransport-Mitarbeiter, etc. nun Berufshelfer sind oder nicht, sowie die Unterscheidung zwischen eigenem Personal und Personal eines Dienstleisters hinfällig. Die Personengruppe „sonstige mitwirkende Person“ umfasst dies alles.

Voraussetzungen sind:

- Die mitwirkende Person muss in die berufliche oder dienstliche Tätigkeit der schweigepflichtigen Person einbezogen bzw. in die Vorbereitung dieser Tätigkeit eingebunden sein. Die Einbeziehung muss im Einvernehmen mit der schweigepflichtigen Person geschehen. Dies gilt auch in mehrstufigen Auftrags- und Unterauftragsverhältnissen.
- Das Offenbaren muss für die Inanspruchnahme der Leistungen der mitwirkenden Person erforderlich sein. Werden darüber hinaus weitere Geheimnisse offenbart, macht der Berufsgeheimnisträger sich strafbar. Seitens des Gesetzgebers gibt keine Einschränkung ob, externe Dienstleister werden können.
- Der Berufsgeheimnisträger ist verpflichtet, dafür Sorge zu tragen, dass die mitwirkenden Personen angemessen zur Verschwiegenheit verpflichtet wird. Andernfalls macht er sich strafbar.
- Das Gleiche gilt für mitwirkende Personen, die wiederum weitere mitwirkende Personen als Unterauftragnehmer einsetzen. Auch sie müssen den Unterauftragnehmer zur Vertraulichkeit verpflichten. Tun sie dies nicht, machen sie sich ebenfalls strafbar.
- Um der aus den letzten zwei Absätzen resultierenden Sorgfaltspflicht zu genügen, muss der Auftraggeber / Verantwortliche den Dienstleister bzw. der Dienstleister die Unterauftragnehmer vertraglich verpflichten, dass die mit der Verarbeitung der durch § 203 StGB geschützten Daten betrauten Beschäftigten auf §203 StGB entsprechend verpflichtet werden. Dieser Passus ist zwingend in den Verträgen erforderlich, da ein Versäumnis strafbewehrt ist.

Für den Abschluss eines AV-Vertrags bedeutet diese neue Regelung im § 203 StGB, dass eine erforderliche Offenbarung nun auch strafrechtlich oftmals zulässig sein kann.

Am 29.06.2017 wurde das Gesetz im Bundestag verabschiedet und vom Bundesrat wurde in der Sitzung vom 22. September 2017 kein Einspruch erhoben. Das Gesetz wurde am 8. November 2018 im Amtsblatt veröffentlicht und trat am Tag nach der Verkündigung in Kraft.[4]

Abgrenzung Funktionsübertragung

Zur Unterscheidung zur Auftragsverarbeitung hat sich aus der Literatur der Begriff der Funktionsübertragung geprägt[5]. Hier werden Daten an den Dienstleister übermittelt, damit dieser in eigener Verantwortung den Auftrag, oftmals eine komplexe Funktion, durchführen kann. Typischerweise führt der Dienstleister die zugehörige Verarbeitung der Daten in eigenen Systemen unter eigener Verantwortung durch. Der Auftraggeber hat also nicht unbedingt Zugriff auf die Verarbeitung.

Da der Dienstleister im Rahmen einer Funktionsübertragung als Dritter anzusehen ist, benötigt der Dienstleister hier auch einen eigenen Erlaubnistatbestand für die Verarbeitung; im Gegensatz zur Auftragsverarbeitung kann er sich hier nicht auf den Erlaubnistatbestand des Auftraggebers stützen. Der Auftraggeber braucht einen Erlaubnistatbestand zur Datenweitergabe an den Dienstleister, der Dienstleister einen (eigenen) Erlaubnistatbestand für die Verarbeitung der Daten.

Beispiele im Gesundheitsbereich hierfür sind Laborbeauftragungen oder Konsile.

Eine neue Regelung in der DS-GVO in Art. 26 DS-GVO kann im Gesundheitsbereich sehr hilfreich sein. Art. 26 DS-GVO kennt „Gemeinsam für die Verarbeitung Verantwortliche“. Wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung festlegen, so sind sie gemeinsam Verantwortliche. In einer Vereinbarung müssen in transparenter Form festgelegt werden, wer welche Verpflichtungen aus der DS-GVO erfüllt. Anwendungsfälle sind hier beispielsweise für ein Medizinisches Versorgungszentrum (MVZ) denkbar, das aus mehreren rechtlich eigenständigen Arztpraxen besteht, die aber gemeinsam einen Patienten behandeln.

Auch für solche Szenarien eignet sich der Muster-AV-Vertrag für das Gesundheitswesen, da entsprechende Passagen hieraus entnommen und entsprechend dem Szenario ergänzt werden können.

Wie auch bei der Funktionsübertragung müssen bei gemeinsam für die Verarbeitung Verantwortlichen die Zulässigkeit einer Datenübermittlung nach der DS-GVO sowie einer Offenbarungsbefugnis im Sinne des § 203 StGB geprüft werden.

Über die Autorin

Barbara Stöferle
ist Sprecherin des AK Medizin.
Die studierte Informatikerin ist seit 1997 als Datenschutzbeauftragte und -beraterin tätig. Sie betreut mehrere Krankenhäuser unterschiedlicher Größe, von Krankenhäusern der Regelversorgung bis zum Klinikum der Maximalversorgung. An der Hochschule Ulm und an der Dualen Hochschule Heidenheim ist sie Lehrbeauftragte für den Datenschutz bzw. medizinischen Datenschutz.

[4] https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3618.pdf%27%5D__1510594994238

[5] Simitis/Dammann/Mallmann/Reh, Kommentar zum Bundesdatenschutzgesetz, Nomos Verlagsgesellschaft, 3. Auflage 1981

https://dipbt.bundestag.de/doc/btd/11/043/1104306.pdf

DER AKTUELLE GESETZESENTWURF ZUM NEUEN SCHWEIZER DATENSCHUTZRECHT (VE-DSG-CH) UNTER VERGLEICHENDER BERÜCKSICHTIGUNG DES NEUEN EUROPÄISCHEN DATENSCHUTZRECHTS (DS-GVO/GDPR)

Marcel Griesinger und Jutta Sonja Oberlin

1. aktuelle Entwicklung im Schweizer Datenschutzrecht

Das Schweizer Datenschutzrecht befindet sich aktuell in der Totalrevision. Neben den Anpassungen des Rechts an die neuen technologischen Gegebenheiten wird durch die Revision auch die Voraussetzung dafür geschaffen, dass die Schweiz seitens der EU auch zukünftig als adäquater Drittstaat mit einem angemessenen Datenschutzniveau anerkannt wird.[1] Dies ist von hervorgehobener Wichtigkeit, damit grenzüberschreitende Datenübertragungen auch weiterhin möglich sind. Dies ist für Schweizer Unternehmen von besonderer Bedeutung.

Der Bundesrat (Regierung) hat im Dezember 2016 den ersten Vorentwurf zum neuen Schweizer Datenschutzgesetz veröffentlicht.[2] Im Rahmen des Gesetzgebungsverfahrens[3] lief die Anhörungsfrist (sog. Vernehmlassung) zum Vorentwurf bis Ende April 2017. Am 15. September wurde nunmehr der Entwurf des Bundesrates (sog. Botschaft) zum Datenschutzgesetz (inkl. weiterer Dokumente) veröffentlicht.[4] Das derzeit geltende Schweizer Datenschutzgesetz (DSG) erfährt danach Änderungen in zentralen Regelungsfeldern. Augenscheinlich ist die Orientierung an der EU-Datenschutzgrundverordnung (DS-GVO)[5], welche das europäische Datenschutzrecht weitgehend vereinheitlicht. Der aktuelle Entwurf zum neuen Datenschutzgesetz wird im nächsten Schritt im Parlament beraten. Seitens des Bundesrats wurde die (optimistische) Hoffnung geäussert, dass das neue DSG-CH bis August 2018 in Kraft treten kann.[6]

2. zentrale Inhalte des Schweizer Vorentwurfs zum Datenschutzgesetz (VE-DSG-CH)

Nachfolgend sollen die zentralen Inhalte und Neuerungen des Vorentwurfs dargestellt werden. Die Zielsetzung der Autoren ist darauf gerichtet, dem Leser einen Überblick über die wesentlichen Regelungspunkte zu geben:

a. Geltungsbereich

Das neue Schweizer Datenschutzgesetz soll ausschliesslich dem Schutz natürlicher Personen dienen. Abweichend vom derzeitigen Datenschutzgesetz sollen Unternehmen zukünftig nicht mehr als Datensubjekt angesehen werden.

b. Strafbestimmungen

Im Gegensatz zu den derzeitigen gesetzlichen Regelungen sieht der VE-DSG-CH empfindliche Geldstrafen bei Datenschutzverletzungen vor. Ursprünglich war vorgesehen, dass Geldstrafen bis zu einer Höhe von 500.000 CHF ausgesprochen werden können. Der Strafrahmen wurde im vorliegenden VE-DSG-CH jedoch auf eine Höchststrafe von 250.000 CHF abgesenkt, um die zahlreichen kritischen Stimmen zu besänftigen.[7]

c. Ausweitung des Rechts von Individualpersonen

Informations- und Kontrollrechte: Das neue Schweizer Datenschutzgesetz beinhaltet zum einen ein erheblich ausgeweitetes Informationsrecht des Einzelnen, wodurch eine spürbar erhöhte Transparenz in der Datenverarbeitung bewirkt werden soll.[8] Zum anderen hat der Gesetzesentwurf auch deutlich verbesserte Kontrollrechte. [9]

Informationspflicht bei automatisierter Datenverarbeitung: Das neue Recht sieht in Art. 15 VE-DSG-CH eine Informationspflicht bei vollständig automatisierten Einzelentscheidungen vor. Die betroffene Individualperson ist, im Fall einer Datenauswertung ohne menschlichen Einfluss, zu informieren, wenn durch den Vorgang eine Entscheidung getroffen wird, die eine rechtliche Auswirkung auf die betroffene Person hat (bspw. die Entscheidung über die Kreditwürdigkeit).

Auskunftsrecht und „Recht auf Vergessen werden“: Die Gesetzesvorlage beinhaltet zudem in Art. 25 VE-DSG das Recht des Datensubjekts Auskunft hinsichtlich seiner Daten zu verlangen. Darüber hinaus kann der Betroffene nunmehr auch die Löschung ihn/sie betreffende personenbezogene Daten verlangen.[10]

„Recht auf Vergessen werden“ für Verstorbene: Das Recht auf Löschung personenbezogener Daten soll zukünftig nicht mehr nur für lebende Personen gelten, sondern vielmehr auch für verstorbene Personen, Art. 12 VE-DSG-CH.

d. Deutliche Ausweitung der Pflichten für Unternehmen

Datenschutzfolgeabschätzung (DPIA): In Abweichung zum aktuellen DSG-CH sieht Art. 16 VE-DSG-CH zukünftig das Erfordernis einer Datenschutzfolgeabschätzung vor. Dabei handelt es sich um eine Risikobeurteilung der Auswirkungen eines Datenbearbeitungsvorgangs auf die Privatsphäre des betroffenen Datensubjekts. Nach Art. 20 Abs. 3 VE-DSG-CH enthält die Folgenabschätzung „eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.“ Eine solche Folgeabschätzung ist indes nur bei „hohen“ Risiken verpflichtend vorgeschrieben, vgl. Art. 20 Abs. 1 VE-DSG-CH. In Absatz 2 des Artikels ist eine nicht abschliessende Aufzählung von Fällen enthalten, die ein hohes Risiko i.S.d. Abs. 1 darstellen.

Data Breach Notification: In Art. 22 VE-DSG-CH ist nunmehr die Pflicht zur Meldung von Verletzungen der Datensicherheit geregelt. Das Erfordernis einer solchen Meldung besteht nur bei einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person. Die Meldung hat jedenfalls die Art der Verletzung der Datensicherheit, die Folgen sowie vorgenommene oder beabsichtige Massnahmen zu enthalten.

Privacy by design/Privacy by default: Art. 6 VE-DSG-CH führt den Titel „Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen“. Die Norm gibt vor, dass die Datenbearbeitung technisch und organisatorisch so zu erfolgen hat, dass die Vorschriften zum Datenschutz eingehalten werden. Gleichzeitig wird der Verantwortliche verpflichtet, mittels entsprechender Voreinstellungen ▸

[1] Gleichzeitig soll durch die Revision auch ermöglicht werden, das Datenschutzübereinkommen SEV 108 des Europarats zu ratifizieren.

[2] Guter Überblick hierzu bei: Seiler, siehe https://home.kpmg.com/ch/de/home/themen/2017/03/update-data-protection-act.html, abgerufen 02.10.2017.

[3] Siehe https://www.admin.ch/gov/de/start/bundesrecht/vernehmlassungen.html, abgerufen 02.10.2017.

[4] Vgl. Schweizerische Eidgenossenschaft, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, abgerufen unter: https://www.ejpd.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/bot-d.pdf

[5] Vgl. Schweizerische Eidgenossenschaft, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, vom 15. September 2017.

[6] Vgl. Schweizerische Eidgenossenschaft, Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, vom 15. September 2017.

[7] Vgl. Schweizerische Eidgenossenschaft, Botschaft zum Bundesgesetz über die Totalrevision des Bundes-gesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, vom 15. September 2017.

[8] Art. 20 VE-DSG-CH

[9] Art. 13, 19, 20 VE-DSG-CH

[10] Hierbei sind indes auch die gesetzlichen Verpflichtungen zu beachten: bspw. müssen Banken bestimmte Daten entspr. Art. 962 OR Daten bis zu 10 Jahre aufbewahren (Aufbewahrungsfristen auch in Art. 2 Abs. 3 GwG definiert). In diesem Fall kann dem Löschungsbegehren erst nach Ablauf dieser gesetzlichen Frist entsprochen werden.

DATENSCHUTZPRAXIS

sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist.

Dokumentation: Weiterhin ist in Art. 11 VE-DSG-CH die Verpflichtung zur Führung eines Verzeichnisses der Bearbeitungstätigkeit niedergelegt.[11]

Erhöhte Transparenzpflichten: u.a. ist in Art. 17 VE-DSG-CH die Informationspflicht bei der Beschaffung von Personendaten geregelt (Ausnahmen hierzu in Art. 18 VE-DSG-CH). Zudem ist der Betroffene im Fall automatisierter Einzelfallentscheidungen nach Art. 19 VE-DSG-CH über die Entscheidung zu informieren, wenn sie mit einer Rechtsfolge verbunden ist oder den Betroffenen erheblich beeinträchtigt.

e. Stärkung der Bedeutung staatlicher Stellen

Durch den neuen Gesetzesentwurf wird schliesslich eine deutliche Stärkung der Stellung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) bewirkt.

Nach dem derzeit geltenden Recht sind die Möglichkeiten des EDÖB darauf beschränkt, gegenüber Unternehmen blosse Empfehlungen abzugeben. Der Gesetzesentwurf erweitert die Befugnis des EDÖB insoweit, dass er danach von Amts wegen oder auf Anzeige hin Untersuchungen eröffnen kann, es ihm ermöglicht wird, erforderlichenfalls vorsorgliche Massnahmen anzustrengen und nach Untersuchungsabschluss sogar Verfügungen erlassen kann. Anzumerken ist indes, dass der EDÖB auch weiterhin keine (Verwaltungs-)Sanktionen erlassen kann. Der Gesetzgeber hat die Zuständigkeit hierfür weiterhin der Gerichtsbarkeit zugewiesen.

f. sonstiges

Zertifizierung: Nach Art. 10 VE-DSG-CH sollen die Hersteller von Datenverarbeitungssystemen oder -programmen ihre Systeme, Produkte und Dienstleistungen zukünftig zertifizieren lassen können.

[11] Siehe auch Art. 11 Abs. 2 VE-DSG-CH zur Konkretisierung der Dokumentationspflichten.

[12] Und, wie wir meinen, wenig aussagekräftig.

3. Vergleich des VE-DSG-CH mit der Datenschutzgrundverordnung (DS-GVO) - wesentliche Abweichungen / andere Regelungen

Das VE-DSG-CH ist grundsätzlich mit ähnlichen, bis sogar deckungsgleichen Grundsätzen und Regelungen wie die DS-GVO versehen. Indes bestehen auch Abweichungen. Die zentralen Unterscheidungen werden im Folgenden überblicksmässig beschrieben.

Der Schweizer Gesetzgeber sieht keinen exterritorialen Anwendungsbereich des in der Revision befindlichen Gesetzes vor, was bedeutet, dass das zukünftige Schweizer Datenschutzgesetz nur innerhalb des Schweizer Staatsgebiets Anwendung findet und nicht auf die generelle Verarbeitung personenbezogener Daten von Schweizer Bürgern auch im Ausland abzielt. Dies stellt eine Abweichung von der EU Regelung dar, für welche der exterritoriale Anwendungsbereich eine der wichtigsten Neuerungen ab Mai 2018 darstellt. Seitens der EU wird damit darauf abgezielt, dass in Zukunft alle sich in der EU befindenden Personen im Fall einer Datenbearbeitung ihrer personenbezogenen Daten aus dem (Nicht-EU)Ausland heraus ebenfalls geschützt werden sollen.

Zudem hat der Schweizer Gesetzgeber auf das Recht der Datenportabilität verzichtet, was sich besonders für mittelständische Schweizer Unternehmen als positiv verzeichnen lässt. Das Recht auf Datenportabilität lässt für die Zukunft einen erheblichen Aufwand für die zur Umsetzung verpflichteten Unternehmen erwarten. Die DS-GVO beschreibt selbst jedoch keinen genauen Prozess, wie die Datenportabilität konkret zu erfolgen hat. Vielmehr bezeichnet die Verordnung das Vorgehen hierzu schlicht dergestalt[12], dass dieses gemäss Art. 20 DS-GVO vom Verantwortlichen in einem „strukturierten, gängigen und maschinenlesbarem Format“ umgesetzt werden muss.

Die Bussgelder können in der DS-GVO bis hin zu 4% des globalen Jahresumsatzes der ganzen Gruppe oder 20`000`000.- Euro reichen, je nachdem, welcher Betrag der höhere ist. Die Schweizer Regulation beschränkt sich hierbei auf 250`000.- CHF.

Im Vergleich zur DS-GVO, in welcher gemäss Art. 37 DS-GVO ein Datenschutzbeauftragter unter bestimmten Voraussetzungen ernannt werden muss, begnügt sich das VE-DSG-CH mit der freiwilligen Ernennung eines Datenschutzberaters. Die freiwillige Ernennung führt jedoch zu einer Privilegierung bei den Datenschutz-Folgeabschätzungen. Die Privilegierung besteht darin, dass hier der EDÖB sodann nicht mehr konsultiert werden muss.

Neu führt das VE-DSG-CH auch eine Regelung ein, welche in der DS-GVO gänzlich fehlt. Dies ist das Recht auf Löschung von Daten Verstorbener. So schützt der Schweizer Gesetzgeber auch die Daten von Verstorbenen und räumt Interessengruppen, wie z.B. der Familie, diese Rechte ein.

Für den Anwender in der Rechtspraxis ist darüber hinaus die Regelung des Art. 59 VE-DSG-CH von entscheidender Bedeutung. Art. 59 VE-DSG-CH regelt u.a., dass die Verantwortlichen sowie die Auftragsbearbeiter zwei Jahre nach Inkrafttreten des Gesetzes in der Lage sein müssen, eine Datenschutz-Folgenabschätzung nach Artikel 16 vorzunehmen.

4. Conclusio und Zusammenfassung

Der nunmehr vorliegende Entwurf zum Schweizer DSG beinhaltet – obgleich der vorstehend dargestellten Abweichungen - eine sehr starke Angleichung an die Anforderungen der europäischen Datenschutzgrundverordnung. Der Gesetzesentwurf muss nun in einem nächsten Schritt die parlamentarische Hürde überspringen. Ob sich in diesem Zusammenhang weitere Änderungen ergeben, bleibt abzuwarten. Darüber hinaus ist auch nicht auszuschliessen, dass der Gesetzesentwurf noch „vor's Volk“ kommt, also im Rahmen einer Volksabstimmung über das neue Schweizer Datenschutzgesetz entschieden wird.

Über die Autoren

Marcel Griesinger
Rechtsanwalt bei KPMG im Team IT Advisory, Schwerpunkt in der Beratung im Wirtschafts- und Datenschutzrecht sowie im Bereich Compliance

Jutta Sonja Oberlin
CIPM, Compliance Officer Univ. (Universität Augsburg), Deutsche Datenschutzbeauftragte (TÜV) ist Senior Consultant bei der KPMG AG in Zürich und berät hier als Datenschutzexpertin im IT Advisory Team

DIE VERTRAUENSWÜRDIGE VERTEILUNG VON VERSCHLÜSSELUNGSSCHLÜSSELN ALS HEMMSCHUH DER E-MAIL-VERSCHLÜSSELUNG – EIN LÖSUNGSANSATZ[1]

Stephan Blazy, Susan Gonscherowski,
Thomas Kunz, Annika Selzer, Ulrich Waldmann

1. Was ist das Problem?

Möchte der Sender einer E-Mail eine Information verschlüsselt an den E-Mail-Empfänger senden, so benötigt der Sender den öffentlichen Schlüssel des Empfängers in Form eines digitalen Zertifikats (im Folgenden: Zertifikat). Ein Zertifikat bescheinigt die Vertrauenswürdigkeit eines öffentlichen Schlüssels und enthält neben dem öffentlichen Schlüssel i. d. R. auch personenbezogene Daten, wie z. B. den Namen und die E-Mail-Adresse des Zertifikatinhabers.[2] Mit dem öffentlichen Schlüssel wird die Information verschlüsselt, d. h. in einen Geheimtext überführt, dann an den Empfänger versandt und mit Hilfe seines privaten Schlüssels wieder in den Klartext versetzt bzw. entschlüsselt. Die Sicherheit des Verfahrens hängt dabei auch vom verantwortungsvollen Umgang mit dem privaten Schlüssel ab, der - im Gegensatz zum öffentlichen Schlüssel - nur dem Zertifikatsinhaber bekannt sein darf.[3]

Problematisch ist, dass Personen, die über ein kryptographisches Schlüsselpaar verfügen, häufig Schwierigkeiten dabei haben, das Zertifikat ihres Kommunikationspartners aufzufinden. Somit fehlt Personen, die verschlüsselte E-Mails versenden möchten, die grundlegende Information, ohne die eine E-Mail-Verschlüsselung nicht möglich ist.

Um dieses grundlegende Problem der E-Mail-Verschlüsselung zu lösen, arbeitet seit 2016 ein Konsortium aus Industrie und Wissenschaft an dem Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" (VVV).[4]

2. Wie kann das Problem gelöst werden?

Zertifikate können in so genannten Verzeichnisdiensten abgelegt werden, die eine Art „Telefonbuch" für Verschlüsselungsschlüssel darstellen. Der Sender einer Information kann in einem solchen Verzeichnisdienst – z. B. durch die Eingabe der E-Mail-Adresse des Empfängers – nachschauen, ob sein gewünschter Kommunikationspartner sein Zertifikat in dem Verzeichnisdienst hinterlegt hat. Die Nutzung von Verzeichnisdiensten stellt Nutzer in der Praxis jedoch vor Probleme. Hinzu kommt, dass die beiden verbreitetsten Verfahren zur E-Mail-Verschlüsselung, S/MIME und OpenPGP, hinsichtlich der eingesetzten Schlüsselformate und Vertrauensmodelle nicht zueinander kompatibel sind. Beide Verfahren sind hinsichtlich der Schlüsselverteilung kompliziert und wenig benutzungsfreundlich.

So stellen S/MIME-Verzeichnisdienste i. d. R. „isolierte Insellösungen" dar, d. h. sie sind nicht miteinander verbunden und jeder Nutzer kann in seinem E-Mail-Client nur einen einzigen Verzeichnisdienst einstellen. Ist in diesem Verzeichnisdienst das Zertifikat des gewünschten Kommunikationspartners nicht auffindbar, so wird das Zertifikat nicht automatisch in allen weiteren bekannten Verzeichnisdiensten gesucht. Dies ist in etwa vergleichbar mit der Reichweite gedruckter Telefonbücher für einzelne Städte im Gegensatz zu der Onlinevariante eines Telefonbuches, in dem Telefonnummern weltweit gesucht werden können.

Beim OpenPGP-Standard stellt sich wiederum das Problem, dass Verzeichnisdienste zwar untereinander synchronisiert werden, dieser Umstand jedoch u. a. dazu führt, dass ein Zertifikat nicht mehr manuell durch den Nutzer gelöscht werden oder korrigiert werden kann bzw. nicht (gut) überprüfbar ist, ob eine Veröffentlichung tatsächlich von dem Berechtigten selbst autorisiert wurde oder welches der veröffentlichten Zertifikate (noch) aktuell ist.

Diese wenig praktikablen Lösungen sollten durch ein für OpenPGP und S/MIME einheitliches und benutzerfreundliches Verfahren zum Auffinden von Zertifikaten abgelöst werden. Genau dies hat sich das Projekt VVV zum Ziel gesetzt.

3. Wie ist die Lösung technisch ausgestaltet?

VVV macht es möglich, von einer E-Mail-Adresse auf den Speicherort eines dazu gehörigen Zertifikats zu schließen. Jeder Nutzer veröffentlicht sein Zertifikat auf einem Schlüsselserver seines E-Mail-Anbieters. Die Adresse des Schlüsselservers wird auf dem DNS-Server der Mail-Domain in Form eines „Service Resource Records" hinterlegt. Dieser Resource Record ist mittels DNS Security Extensions" (DNSSEC) geschützt, konkret durch eine DNSSEC-Signatur des E-Mail-Anbieters, dessen Signaturschlüssel wiederum vom darüber liegenden Domain-Inhaber signiert wurde usw. bis hin zur Signatur der Root-Domain des DNS. Auf diese Weise entsteht eine eindeutige Vertrauenskette von signierten Schlüsseln der Domain-Inhaber auf Basis eindeutiger Instanzen (bestimmt durch die E-Mail-Domain) und einer einzigen Root-Domain. Die E-Mail-Anwendung überprüft die Authentizität der Resource Records durch die Validierung der DNSSEC-Signaturen. Der E-Mail-Anbieter hat die entscheidende Rolle inne, da er für die Zuordnung von den Schlüsseln zu den E-Mail-Adressen der Nutzer bürgt. Damit brauchen die Nutzer nur solchen Instanzen zu vertrauen, denen sie beim Gebrauch von E-Mail-Adressen ohnehin vertrauen: Den Betreibern der grundlegenden Internetdienste (DNS) und den E-Mail-Anbietern.

Die beiden wichtigsten Anwendungsfälle der Schlüsselverteilung sind das Veröffentlichen und das Abrufen von Schlüsseln. Nutzer veröffentlichen mit Hilfe des VVV-Verfahrens ihre eigenen Zertifikate. Sie werden mittels der VVV-Lösung für andere Nutzer automatisch abrufbar, so dass sich alle Nutzer die Schlüssel ihrer Kommunikationspartner leicht beschaffen können.

Veröffentlichung von Schlüsseln: Zur Veröffentlichung des Zertifikats weist der Nutzer gegenüber dem E-Mail-Anbieter nach, dass er auf das E-Mail-Postfach Zugriff hat. Die E-Mail-Anwendung vermittelt die Nutzer-Authentifizierung und sendet nach erfolgreicher Authentifizierung das ausgewählte Zertifikat zur Veröffentlichung an den E-Mail-Anbieter. Der Nutzer muss nun den Besitz des zugehörigen privaten Schlüssels nachweisen. Dazu verschlüsselt der E-Mail-Anbieter mit dem empfangenen öffentlichen Schlüssel einen Verifikationscode. Nach erfolgreicher Entschlüsselung sendet die Anwendung den Verifikationscode an den E-Mail-Anbieter zurück, der den Schlüssel auf einem seiner Schlüsselserver veröffentlicht. Der Nutzer kann ein veröffentlichtes Zertifikat jederzeit aktualisieren oder auch ersatzlos löschen.[5]

Abruf von Schlüsseln: Der Nutzer verfasst in seiner E-Mail-Anwendung eine E-Mail und hat die E-Mail-Verschlüsselung aktiviert. Sobald er eine vollständige E-Mail-Adresse in das Empfängerfeld eingetragen hat, sucht die Anwendung mit der E-Mail-Adresse nach dem entsprechenden Zertifikat des Empfängers. ▶

[1] Dieser Beitrag entstand im Rahmen des Projekts „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln (VVV)" (https://keys4all.de), das vom Bundesministerium für Bildung und Forschung unter dem Förderkennzeichen 16KIS0354K gefördert wird.

[2] Es ist jedoch grundsätzlich auch möglich, dass das Zertifikat neben dem öffentlichen Schlüssel lediglich pseudonymisierte Daten wie z. B. eine pseudonyme E-Mail-Adresse enthält. Dieser Fall steht jedoch nicht im Fokus dieser Ausarbeitung.

[3] Herfert/Selzer/Waldmann, Selbstdatenschutz in Zeiten massenhafter E-Mail-Überwachungen, in: BvD-News 01/2016, S. 57-59.

[4] Für nähere Details zu den in diesem Artikel beschriebenen Projektergebnissen vgl. Blazy/Gonscherowski/Selzer, Anforderungen des künftigen europäischen Datenschutzrechts an die vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln und Fischer/Kunz/Lorenz/Waldmann, Verfahren zur vertrauenswürdigen Verteilung von Verschlüsselungsschlüsseln, beides in: Eibl/Gaedke (Hrsg.): INFORMATIK 2017, Lecture Notes in Informatics (LNI), Bonn 2017. Beide Veröffentlichungen können über die Projekt-Webseite www.keys4all.de abgerufen werden.

[5] Das Löschen könnte aus verschiedenen Gründen vom Nutzer gewollt sein, beispielsweise weil der private Schlüssel kompromittiert wurde oder weil der Nutzer mit seiner E-Mail-Adresse nicht mehr in einem offen zugänglichen Verzeichnis stehen möchte. Das Löschen ist also nicht unbedingt mit einem Widerruf des Schlüssels gleichzusetzen.

DATENSCHUTZPRAXIS

Dazu ruft die Anwendung vom DNS-Server des E-Mail-Anbieters des Empfängers den entsprechenden Resource Record ab und überprüft die DNSSEC-Signaturen dieses Records. Konnten die Server-Adressen auf diese Weise verifiziert werden, so ruft die Anwendung anhand der E-Mail-Adressen auf den Schlüssel-Servern die Schlüssel der Empfänger ab. Schließlich wird die E-Mail für die Empfänger verschlüsselt und abgesendet.

4. Was muss die Lösung aus Sicht des Datenschutzes beachten?

Die im VVV-Projekt entwickelte Anwendung stellt dem Nutzer über eine Anwendung die Zertifikate der Kommunikationspartner zur Verfügung. Die im Zertifikat aufgeführten Daten wie Name, Vorname sowie weitere Angaben, etwa Anschrift oder E-Mail-Adresse – OpenPGP erlaubt gar das Einfügen von Gesichtsbildern – stellen personenbezogene Daten dar. Beabsichtigt der E-Mail-Anbieter nun im Rahmen einer Public-Key-Infrastruktur diese Zertifikate zu verwalten und zu verteilen, sind die einschlägigen datenschutzrechtlichen Regelungen zu beachten.

Über die o. g. Anwendung können Inhalte über die Anwendung in Verzeichnisse veröffentlicht und auch aus elektronischen Verzeichnissen abgerufen werden. Es handelt sich entsprechend um einen Telemediendienst, der es dem Nutzer ermöglicht ein Zertifikat in einem Verzeichnis eines E-Mail-Übertragungsdienstes bereitzustellen. E-Mail-Übertragungsdienste gehören zur Kategorie interpersoneller Kommunikationsdienste, wie sie in Art. 2 Abs. 5 im Entwurf der Richtlinie des Europäischen Parlaments und des Rates über den europäischen Kodex für die elektronische Kommunikation definiert sind. Dieser Definition folgt auch der Entwurf der e-Privacy-VO.

Art. 15 e-Privacy-VO-E befasst sich mit der Regelung öffentlich zugänglicher Verzeichnisse. Die Hinterlegung des einem Endnutzer zugeordneten Zertifikats in ein providerseitiges Verzeichnis und die Möglichkeit der öffentlichen Abfrage dieser Information mit dem Zweck der Kontaktaufnahme fällt in den Anwendungsbereich des Verordnungsentwurfs. Dies hätte zu Folge, dass die E-Mail-Anbieter von dem Nutzer als Betroffenen gem. Art. 15 Abs. 1 e-Privacy-VO-E die ausdrückliche Einwilligung in die Aufnahme des Verzeichnisdienstes einzuholen verpflichtet sind. Neben der Aufnahme erstreckt sich die Einwilligung auch auf die Suchfunktionalitäten, über die der Nutzer im Vorhinein aufzuklären ist. Den Nutzern – unabhängig ob sie nun natürliche oder juristische Personen sind – wird darüber hinaus nach Art. 15 Abs. 4 e-Privacy-VO-E das Recht eingeräumt ihre Zertifikate kostenlos auf ihre Richtigkeit hin zu überprüfen und ggf. zu löschen. Zusätzlich sind eine Fülle von Vorgaben gem. DS-GVO einzuhalten. Hierzu zählen u. a.:

Rechtmäßigkeit der Verarbeitung: Die Zertifikate des Nutzers werden vom Anbieter gespeichert und bei entsprechenden Anfragen an die jeweiligen Kommunikationsteilnehmer übermittelt. Diese Verwaltung der Zertifikate beim Anbieter stellt eine Verarbeitung i. S. d. Art. 4 Nr. 2 DS-GVO dar und muss für eine rechtliche Legitimation einen Tatbestand des Art. 6 Abs. 1 UAbs. 1 DS-GVO erfüllen. Hat der Nutzer einen Account bei einem E-Mail-Anbieter, liegt als Rechtsgrundlage bereits ein Vertrag mit dem Anbieter i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO vor. Das Hochladen des eigenen Zertifikats mit einem vom E-Mail-Anbieter bereitgestellten Verfahren kann in diesem Fall als konkludente Vertragserweiterung angesehen werden, auf welche die Verarbeitung gestützt werden kann. Die Verarbeitung personenbezogener Daten Dritter, z. B. in Form eines signierten Schlüssels, ist jedoch nicht vertraglich erfasst.[6]

Datenminimierung: In den in Art. 5 DS-GVO normierten Grundsätzen der Datenverarbeitung ist in Art. 5 Abs. 1 lit. c DS-GVO die Datenminimierung festgeschrieben. Hiernach muss die Verarbeitung personenbezogener Daten dem Zweck angemessen, erheblich sowie auf das notwendige Maß begrenzt sein.

Datenrichtigkeit und Löschung: Gem. Art. 15 und 16 DS-GVO muss der E-Mail-Anbieter eine Überprüfung („Auskunftsrecht") und Berichtigung („Recht auf Berichtigung") personenbezogener Daten ermöglichen. Korrespondierend normiert Art. 17 Abs. 1 DS-GVO den Anspruch der betroffenen Person auf Löschung ihrer sämtlichen personenbezogenen Daten. Dieses „Recht auf Vergessenwerden" greift in den Fällen, in denen die Daten für die ursprüngliche Zweckerreichung nicht mehr notwendig sind, der Betroffene seine Einwilligung widerruft, die Befristung ausläuft, der Verarbeitung widersprochen wird bzw. diese mit der DS-GVO nicht vereinbar ist.

Informationspflichten: Zu den Informationspflichten eines E-Mail-Anbieters gehören hauptsächlich Aufklärung, Auskunft und Benachrichtigung der Nutzer. Die DS-GVO stellt auf eine umfassende Informiertheit des Betroffenen ab. Die Pflichten des Verantwortlichen gegenüber dem Betroffenen gelten unabhängig davon, ob die Erhebung direkt bei der Person oder an anderer Stelle stattfindet. Jedoch erweitert Art. 14 Abs. 1 und Abs. 2 litt. a-d DS-GVO in diesem Fall den Umfang der Informationspflichten.

Datensicherheit: Die E-Mail-Anbieter müssen auch für die Sicherheit der ihnen überantworteten personenbezogenen Zertifikatsinformationen Sorge tragen. Den Rahmen hierfür geben Art. 5 Abs. 1 lit f und Art. 32 DS-GVO vor.

Nachweis-/Rechenschaftspflichten und Haftung der E-Mail-Anbieter: Art. 82 Abs. 2 DS-GVO besagt: Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechenden Verarbeitung verursacht wurde.[7] In Art. 5 Abs. 2 DS-GVO legt der Gesetzgeber ausdrücklich fest, dass der Verantwortliche die Einhaltung der Bestimmungen aus Art. 5 Abs. 1 DS-GVO nachweisen können muss. Entsprechend dieser Gesetzeslage kann eine betroffene (natürliche) Person Schadenersatz verlangen, wenn der E-Mail-Anbieter nicht nachweisen kann, dass die Verarbeitungsgrundsätze der Verordnung eingehalten wurden. Zu den Nachweispflichten gegenüber der Aufsichtsbehörde zählen die Verfahrensnachweise bzw. Datenschutz-Folgenabschätzungen (Art. 35 DS-GVO) und Meldungen von Verletzungen des Schutzes personenbezogener Daten gem. Art. 33 DS-GVO. Mit Art. 24 DS-GVO erfolgt eine Umkehrung der Beweislast zu Gunsten des Betroffenen.

5. Wie ist der Stand der Umsetzung?

Das Projekt „Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln" (VVV) wird unter der Leitung von Fraunhofer SIT gemeinsam mit der Universität Kassel (provet), der Universität der Künste Berlin, mailbox.org und dem Unabhängigen Landeszentrum für Datenschutz (ULD) bearbeitet.

Da die E-Mail-Anwendung aus Nutzersicht die zentrale Komponente der E-Mail-Kommunikation ist, implementiert das Konsortium das VVV-Verfahren derzeit beispielhaft in Form einer Erweiterung (Plugin) der E-Mail-Anwendung Thunderbird und nutzt die DNS- und Schlüsselserver des E-Mail-Anbieter mailbox.org. Gemeinsam mit mailbox.org führt das Fraunhofer SIT die Implementierungsarbeiten durch und verantwortet darüber hinaus die IT-Sicherheit des VVV-Verfahrens. Die Projektgruppe provet der Universität Kassel und das Unabhängige Landeszentrum für Datenschutz begleiten das Projekt aus verfassungsrechtlicher sowie datenschutzrechtlicher Sicht. Die Universität der Künste bezieht unterschiedliche Nutzergruppen in allen Phasen des Entwicklungsprozesses mit ein, um Anforderungen für das Bedienkonzept des Plugins zu ermitteln.

Über die Autoren

Stephan Blazy
Universität Kassel (Provet)
▶ s.blazy@uni-kassel.de

provet

Susan Gonscherowski
Unabhängiges Landeszentrum für Datenschutz
▶ sgonscherowski@datenschutzzentrum.de

ULD

Thomas Kunz
Fraunhofer SIT, Darmstadt
▶ thomas.kunz@sit.fraunhofer.de

Annika Selzer
Fraunhofer SIT, Darmstadt
▶ annika.selzer@sit.fraunhofer.de

Ulrich Waldmann
Fraunhofer SIT, Darmstadt
▶ ulrich.waldmann@sit.fraunhofer.de

Fraunhofer SIT

[6] Mommers, BGH präzisiert Zulässigkeit von Deep-Links, in: DFN-Infobrief Recht 1/11, 2011.

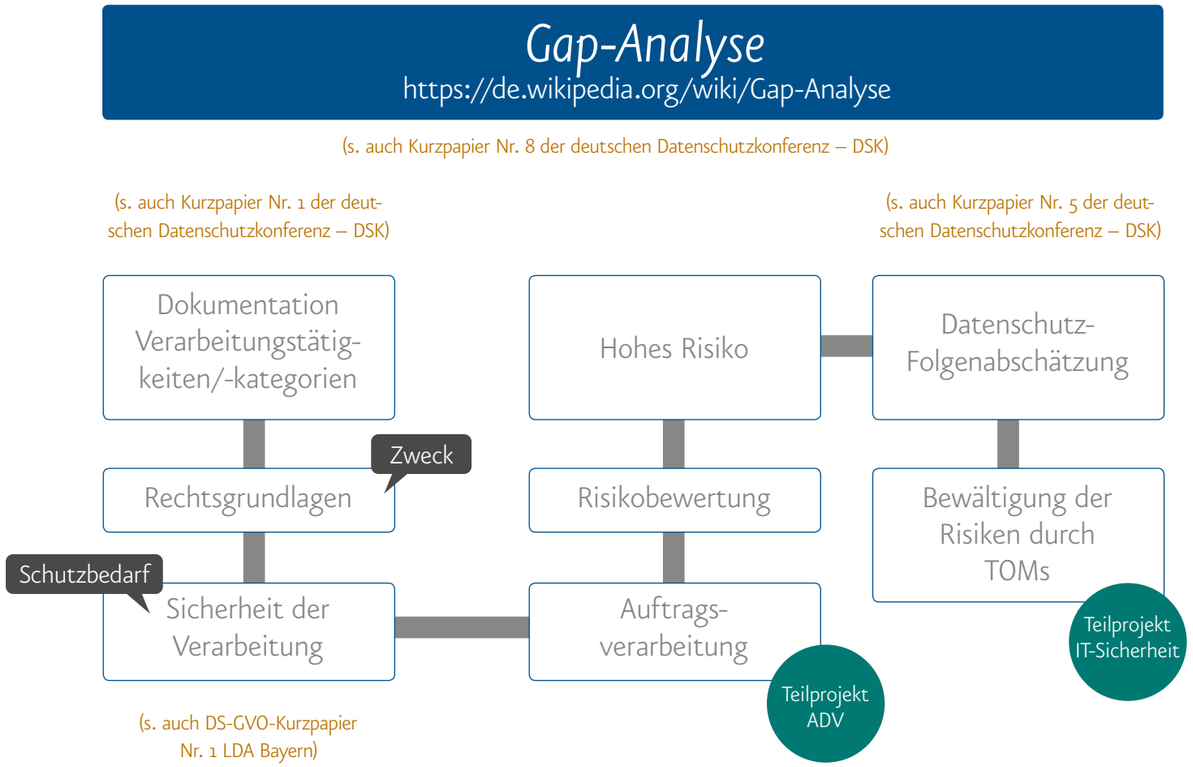
[7] Die Haftung in der e-Privacy-VO-E ist in Art. 22 geregelt und verweist auf die Ausnahmetatbestände des Art. 82 DS-GVO.

SPÄT, ABER NOCH NICHT ZU SPÄT

Evelyn Seiffert

Wer jetzt noch nicht mit dem Anpassungsprozess begonnen hat, dem läuft die Zeit davon. Wer dieses Thema auf die leichte Schulter nimmt (was soll schon passieren), handelt fahrlässig. Es ist nicht auszuschließen, dass die deutschen Aufsichtsbehörden für den Datenschutz relativ frühzeitig nach dem 25.05.2018 Unternehmen und andere Stellen einer ersten Prüfung unterziehen, wie sie den Umstieg auf die neuen Regelungen geschafft haben. Hinzuweisen ist in diesem Zusammenhang auf einen fiktiven Fragebogen des Bayerischen Landesamtes für Datenschutzaufsicht:
https://www.lda.bayern.de/media/DS-GVO_fragebogen.pdf

Die größte Herausforderung für viele Betriebe, gerade für die Unternehmen der mittelständischen Wirtschaft, aber auch für Vereine, Einzelhandel, Freiberufler, Handwerksbetriebe ist die Frage: Wie sollen wir mit dem Thema DS-GVO/BDSG 2018 umgehen und auf welche Weise können wir den „neuen" Anforderungen gerecht werden?



Die neue Gesetzgebung bietet einen guten Anlass, die personenbezogene Datenverarbeitung auf den Prüfstand zu stellen. Zunächst obliegt jedoch der Geschäftsführung, das Projekt DS-GVO/BDSG 2018 zu starten. Dazu gehört, eine Person im Unternehmen für die Steuerung des gesamten Projektes zu benennen. Der betriebliche Datenschutzbeauftragte ist allerdings nicht diese Person, so gern die Geschäftsführung dies auch sehen würde. Der betriebliche Datenschutzbeauftragte ist nicht für die Einhaltung und Umsetzung der datenschutzrechtlichen Anforderungen verantwortlich, war er bisher nicht und ist dies auch in Zukunft nicht (s. Art. 29-Gruppe, WP 243, Kap. 4.1). Er berät das Projekt und kann mit seiner Erfahrung helfen, die richtigen Weichenstellungen vorzunehmen.

Klassische betriebswirtschaftliche Instrumente wie die Gap-Analyse erleichtern die Bestandsaufnahme, die zu Beginn der Überprüfung auf dem Weg vom BDSG zur DS-GVO/zum BDSG 2018 vorzunehmen ist. Der sich daran anschließende Prüfprozess sollte sich zunächst an den Zweckbestimmungen orientieren, die allerdings mit einer Feststellung über die Rechtmäßigkeit der Verarbeitungen verbunden ist. Sofern eine Rechtsgrundlage vorhanden ist, kann der Prüfprozess fortgesetzt werden, andernfalls ist eine möglicherweise zweifelhafte Verarbeitung zu überdenken oder sogar einzustellen.

Mittlerweile wurden zahlreiche Hinweise, Kurzpapiere (s. u.a. Datenschutzkonferenz - DSK, LDA Bayern), Leitfäden, Praxishilfen (z.B. GDD) veröffentlicht. Mit weiteren Hilfen ist auch in den nächsten Monaten verstärkt zu rechnen. Das Rad muss also nicht neu erfunden werden. Betriebe und Unternehmen sind zudem gut beraten, auf bereits bewährte Prozesse und Instrumente zurückzugreifen.

Das Gesamt-Projekt besteht noch aus weiteren Teil-Projekten:

Information/-Benachrichtigung an den Betroffenen	• Wie erfolgte sie bisher? Ausnahmen? • Anpassungsbedarf	(s. auch Kurzpapier Nr. 10 der deutschen Datenschutzkonferenz – DSK)
Betroffenenrechte	• Bisheriges Verfahren, Inhalte • Auskunft • Berichtigung/Widerspruch • Einschränken (Sperren) /Löschen • Datenübertragbarkeit • Anpassungsbedarf	
Datenpannen	• Interner Meldeprozess • Information • Aufsichtsbehörde • Betroffene • Anpassungsbedarf	(s. auch DS-GVO-Kurzpapier Nr. 8 LDA Bayern)

Sofern bei der Bestandsaufnahme Auftragsverarbeitung festgestellt wird, empfiehlt sich, diese Verarbeitungen in das Teilprojekt A(D)V zu verschieben.

Dokumentation zur Vorbereitung Anpassungsbedarf DS-GVO

Auswertung des schriftlichen Auftrages nach Anforderungen des § 11 BDSG												
Auftragnehmer	**Nr.**	**1**	**2**	**3**	**4**	**5**	**5**	**7**	**8**	**9**	**10**	**11.1**	**11.2**

Reglungsinhalte Abs. 2:	Regelungen:
1. Gegenstand und Dauer	**+ = vorhanden**
2. Umfang, Art, Zweck der DV, Art der Daten, Kreis der Betroffenen	**o = teilweise vorhanden**
3. technische und organisatorische Maßnahmen	**- = nicht vorhanden**
4. Berichtigung, Löschung und Sperrung	
5. Pflichten des AN, ins. Kontrollen	
6. Unterauftragsverhältnisse	
7. Kontrollrechte des AG, Mitwirkungspflichten des AN	
8. Verstöße AN nzw. der bei ihm beschäftigten Personen	
9. Umfang Weisungsbefugnisse	
10. Rückgabe Datenträger, Löschung beim AN nach Beendigung	
11. Kontrollkonzept 1. Vor Auftragsvergabe 2 Regelmäßig nach Auftragsvergabe	

Ein erster Abgleich mit den noch geltenden Anforderungen des BDSG und Art 28 DSVGO soll helfen, Prioritäten festzulegen: Welcher Auftrag entspricht dem heutigen Recht? Diese stehen zur Anpassung nicht an erster Stelle. Vielmehr sollte das primär für die Aufträge gelten, die heute schon nicht den Anforderungen genügen.

Bisher veröffentlichte Mustertexte:

- Praxisleitfaden Auftragsverarbeitung IHK Nürnberg (08.2017)

https://www.ihk-nuernberg.de/de/media/PDF/Innovation-Umwelt/Datenschutz-in-der-betrieblichen-Praxis/praxisleitfaden-zur-ds-gvo.pdf

- Mustervertrag DS-GVO (auch in en) (04.2017)

www.gdd.de

- Musterverträge Auftragsverarbeitung Gesundheitswesen DS-GVO (06.2017)

https://www.bvdnet.de/auftragsverarbeitung-im-gesundheitswesen-ein-thema-mit-bisher-vielen-schwierigkeiten/

- Bitkom Auftragsverarbeitung DS-GVO (05.2017)

www.bitkom.org

Fazit:

Wer diesen Prozess der Überprüfung und Anpassung durchführt und das noch vor dem Anwendungsdatum 25.05.2018, hat den Vorteil, die dabei dokumentierten Verarbeitungen zugleich als Nachweis zu nutzen, die die Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO erfüllen hilft.

Über die Autorin

Evelyn Seiffert
ist Diplom-Rechtspflegerin und war von Juni 1992 bis März 2017 beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit tätig. In dieser Zeit prüfte Frau Seiffert eine Vielzahl von Unternehmen unterschiedlicher Branchen, beriet betriebliche Datenschutzbeauftragte, Betriebsräte und Betroffene. Sie ist seit über 15 Jahren als Fachreferentin für Datenschutz bei verschiedenen Veranstaltern mit den Schwerpunkten Datenschutzmanagement/-organisation sowie datenschutzgerechte Geschäftsprozesse tätig. Frau Seiffert ist Autorin des Buches „Datenschutzprüfung durch die Aufsichtsbehörden (nach BDSG)“ sowie Mitautorin der CD-ROM „DS-GVO - Verzeichnis der wichtigen Verarbeitungstätigkeiten“.

Frau Seiffert ist freie Mitarbeiterin bei einer Rechtsanwaltskanzlei.

„DER BEHÖRDLICHE UND BETRIEBLICHE DATENSCHUTZBEAUFTRAGTE NACH NEUEM RECHT“ – HANDREICHUNG DES HESSISCHEN DATENSCHUTZBEAUFTRAGTEN

Yvonne Herzog, Katja Horlbeck

Aufgrund der Europäischen Datenschutzreform erreichen den Hessischen Datenschutzbeauftragten derzeit eine Vielzahl von Anfragen zur Rechtsfigur des Datenschutzbeauftragten nach den Bestimmungen des neuen Rechts[1].

Der Hessische Datenschutzbeauftragte hat daher eine Handreichung erarbeitet, die die Voraussetzungen der Benennung, die persönlichen Anforderungen an den Datenschutzbeauftragten, seine Aufgaben, Pflichten und Stellung vor dem Hintergrund der zukünftigen Regelungen beleuchtet.

Nachfolgend erhalten Sie eine kurze Zusammenfassung der wichtigsten im Arbeitspapier behandelten Punkte:

1) Neue Rechtsvorschriften

Die derzeit noch geltenden Regelungen der §§ 4 f und 4 g BDSG werden mit der unmittelbaren Geltung der DS-GVO ab dem 25.05.2018 abgelöst. Zentrale Regelungen zur Benennung, Stellung und zu den Aufgaben des Datenschutzbeauftragten enthalten sodann die Artikel 37 bis 39 DS-GVO. Zusätzlich sind für betriebliche und behördliche Datenschutzbeauftragte die Vorschriften des BDSG-NEU (§§ 5 bis 7 und 38 BDSG-NEU) und für behördliche weiter die jeweiligen – sich derzeit in Überarbeitung befindlichen – Landesdatenschutzgesetze zu beachten.

2) Neu-Regelung ermöglicht keine erleichterte Abberufung oder Kündigung auf der Grundlage des aktuellen Rechts bestellter Datenschutzbeauftragter

Nach den Vorschriften der §§ 4 f und 4 g BDSG bestellte Datenschutzbeauftragte können in aller Regel nicht mit Verweis auf die neuen gesetzlichen Bestimmungen abberufen oder gekündigt werden, wenn sie die gesetzlichen Anforderungen auch weiterhin erfüllen. Arbeitgeber und Dienstherren müssen ggf. ausreichend Ressourcen (d.h. Fortbildungsmaßnahmen, Lehrmaterial, Zeitschriften etc.) zur Verfügung stellen, damit sich bereits bestellte Datenschutzbeauftragte mit der zukünftigen Rechtslage vertraut machen können.

3) Benennungspflicht

Öffentliche Stellen müssen grundsätzlich einen Datenschutzbeauftragten benennen. Dies ergibt sich aus Artikel 37 Abs. 1 lit. a DS-GVO und aus § 5 Abs. 1 BDSG-NEU. Für betriebliche Datenschutzbeauftragte gilt neben den Tatbestandsvoraussetzungen der Benennung nach Art. 37 Abs. 1 lit. b und c DS-GVO aufgrund der Öffnungsklausel des Artikel 37 Abs. 4 Satz 1 DS-GVO auch weiterhin die quantitative Benennungspflicht bei mehr als zehn beschäftigten Personen, die ständig mit automatisierter Verarbeitung personenbezogener Daten befasst sind. Der deutsche Gesetzgeber hat von der Möglichkeit der Öffnungsklausel des Artikel 37 Abs. 4 Satz 1 DS-GVO Gebrauch gemacht und in § 38 Abs. 1 BDSG-NEU in Ergänzung zu Artikel 37 Abs. 1 DS-GVO weitere Fälle der Pflicht zur Benennung eines Datenschutzbeauftragten normiert.

4) Benennungspflicht für Verantwortliche und Auftragsverarbeiter[2]

[1] D.h. nach den Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, nachfolgend abgekürzt als „DS-GVO“ (Artikel 37 bis 39 DS-GVO) und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, nachfolgend abgekürzt als „JI-RICHTLINIE“ (Artikel 32 bis 34 JI-RICHTLINIE) sowie des Bundesdatenschutzgesetzes, nachfolgend abgekürzt als „BDSG-NEU“ (§§ 5 bis 7, 38 BDSG-NEU).

[2] Vergleiche Artikel 37 Abs. 1 DS-GVO

AUFSICHTSBEHÖRDE

Nach der DS-GVO und dem BDSG-NEU muss sowohl der Verantwortliche als auch der Auftragsverarbeiter einen Datenschutzbeauftragten benennen. Aus deutscher Sicht handelt es sich mithin um eine Erweiterung der bisher bestehenden Bestellpflicht, da Normadressaten des BDSG aktuell nur die verantwortlichen Stellen sind.

5) Veröffentlichungs- und Mitteilungspflicht

Nach Artikel 37 Abs. 7 DS-GVO veröffentlichen Verantwortliche und Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten und teilen diese der Aufsichtsbehörde mit. Den Hessischen Datenschutzbeauftragten erreichen bereits erste Meldungen, mit denen der in Artikel 37 Abs. 7 DS-GVO bestehenden Verpflichtung Rechnung getragen werden soll. Da die Meldepflicht gegenüber den Aufsichtsbehörden erst ab dem 25.05.2018 verpflichtend ist, sollte hiervon aktuell Abstand genommen werden. Der Hessische Datenschutzbeauftragte wird rechtzeitig vor dem 25.05.2018 weitergehende Informationen bezüglich zu meldender Daten und zum Meldeprozess veröffentlichen.

6) „Konzernprivileg" für Benennung[3]

Die DS-GVO ermöglicht Verantwortlichen und Auftragsverarbeitern die Benennung eines Datenschutzbeauftragten für eine Unternehmensgruppe, sofern dieser von jeder Niederlassung leicht erreicht werden kann. Im Verhältnis zur bisherigen Regelung des BDSG handelt es sich somit um eine Erleichterung der formalen Anforderungen, da zukünftig keine separate Bestellung für jedes einzelne Konzernunternehmen mehr erfolgen muss. Der Begriff der leichten Erreichbarkeit verlangt zum einen Sicherstellung der persönlichen Kommunikation durch ausreichend verfügbare Kontaktmöglichkeiten, z.B. die Einrichtung eines Kontaktformulars auf der Webseite, Bereitstellung einer Telefonnummer und/oder E-Mail-Adresse, regelmäßige Sprechstunden für Beschäftigte. Zum anderen muss der Datenschutzbeauftragte in der Lage sein, mit Aufsichtsbehörden und Betroffenen sprachlich zu kommunizieren. Wenn nach deutschem Recht eine Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten besteht, kann somit ein Konzerndatenschutzbeauftragter auch außerhalb Deutschlands für deutsche Niederlassungen benannt werden. Entscheidend ist, dass der Datenschutzbeauftragte aufgrund seiner Eigenschaften sowie seiner Stellung im Unternehmen tatsächlich in der Lage ist, für Betroffene und Aufsichtsbehörden persönlich als Ansprechpartner zur Verfügung zu stehen, d.h., mit ihnen zu kommunizieren und zu kooperieren und die ihm von der DS-GVO auferlegten Aufgaben zu erfüllen.

7) Interne oder externe Benennung möglich[4]

Der Datenschutzbeauftragte kann sowohl Beschäftigter des benennpflichtigen Unternehmens sein als auch auf der Grundlage eines Dienstleistungsvertrages tätig werden. Diese Wahlfreiheit ist für Unternehmen aktuell bereits gegeben, für öffentliche Stellen wird sie durch die Vorschriften der DS-GVO und des BDSG-NEU eingeführt.

8) Datenschutzteam und Benennung juristischer Personen

Neben der Benennung einer einzelnen Person ist es auch möglich, dass mehrere Personen gemeinsam die Aufgaben des Datenschutzbeauftragten wahrnehmen. Nach Ansicht der WP 29[5] ist auch die Benennung einer juristischen Person zum Datenschutzbeauftragten zulässig.[6] Die deutschen Aufsichtsbehörden vertreten hierzu aktuell noch unterschiedliche Auffassungen. Solange eine verbindliche Klärung durch den Europäischen Datenschutzausschuss nicht stattgefunden hat, wird empfohlen, die Benennung einer juristischen Person zum Datenschutzbeauftragten vorab mit der zuständigen Datenschutzaufsichtsbehörde abzustimmen.

9) Freiwillige Benennung

Im Falle der freiwilligen Benennung gelten die Vorschriften des vierten Abschnitts der DS-GVO.[7] Zu beachten ist aber, dass die zur DS-GVO hinzutretenden Privilegien des BDSG-NEU (Abberufungs- und Kündigungsschutz, Verschwiegenheit und Zeugnisverweigerungsrecht) nach dem Wortlaut des § 38 Abs. 2 BDSG-NEU nur bei der verpflichtenden Bestellung zur Anwendung gelangen.

10) Persönliche Anforderungen an den Datenschutzbeauftragten[8]

Sowohl die DS-GVO als auch das BDSG-NEU verlangen, dass der Datenschutzbeauftragte auf der Grundlage der folgenden drei Voraussetzungen benannt wird:

1. berufliche Qualifikation,
2. Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis,
3. Fähigkeit zur Erfüllung der in der DS-GVO bzw. BDSG-NEU genannten Aufgaben.

Zu fordern sind hiernach jedenfalls Kenntnisse des nationalen und Europäischen Datenschutzrechts und ein vertieftes Verständnis der DS-GVO, wobei sich das konkret zu fordernde Fachwissen an der Sensitivität, Komplexität und dem Umfang der Verarbeitungsvorgänge orientieren sollte. Neben der beruflichen und der fachlichen Qualifikation verlangt die WP 29 im Zusammenhang mit der Fähigkeit zur Erfüllung der in der DS-GVO genannten Aufgaben, dass der Datenschutzbeauftragte ein hohes Maß an persönlicher Integrität und Berufsethik mit sich bringen muss.[9]

11) Aufgaben und Pflichten[10]

Bei einer Gesamtschau der Regelungen der DS-GVO sowie des BDSG-NEU lassen sich die folgenden Kernaufgaben für Datenschutzbeauftragte zusammenfassen:

1. Unterrichtung und Beratung,
2. Überwachung der Einhaltung der DS-GVO und anderer Datenschutzvorschriften der Union bzw. der Mitgliedsstaaten (oder des BDSG-NEU und sonstiger Vorschriften über den Datenschutz)/Zuweisung von Zuständigkeiten,
3. Sensibilisierung und Schulung,
4. Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung,
5. Zusammenarbeit mit der Aufsichtsbehörde,
6. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

Die DS-GVO bzw. das BDSG-NEU beschreibt nicht nur einen Aufgabenkatalog, sondern gibt dem Datenschutzbeauftragten auch gleich eine Maxime zur Aufgabenerfüllung an die Hand: Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art und den Umfang, die Umstände und Zwecke der Verarbeitung berücksichtigt.

Daneben steht es Behörden und Unternehmen frei, die Rolle des Datenschutzbeauftragten strategischer und proaktiver auszugestalten als dies in der DS-GVO und dem BDSG-NEU vorgesehen ist. Die Vorschriften enthalten keine abschließende Aufgabenzuweisung.

12) Stellung des Datenschutzbeauftragten[11]

Die unabhängige und organisatorisch herausgehobene Stellung des Datenschutzbeauftragten ist für eine wirkungsvolle Tätigkeit von ausschlaggebender Bedeutung, da er andernfalls den zuvor beschriebenen Aufgaben und Pflichten nur schwerlich gerecht werden kann.[12]

Folgende Themenkreise zur Stellung des Datenschutzbeauftragten in Behörden und Unternehmen können zusammengefasst werden:

[3] Vergleiche Artikel 37 Abs. 2, Abs. 3 DSGVO und § 5 Abs. 2 BDSG-NEU

[4] Vergleiche Artikel 37 Abs. 6 DS-GVO, § 5 Abs. 4 BDSG-NEU, sowie § 4 f Abs. 2 Satz 3 und 4 BDSG

[5] Zu den genannten Rechtsvorschriften hat die Artikel 29 Datenschutzgruppe, hier abgekürzt als „WP 29" bereits im Dezember 2016 das Working Paper 243 „Guidelines on Data Protection Officers ('DPOs')" veröffentlicht. Die Artikel 29 Datenschutzgruppe ist das unabhängige Beratungsgremium der EU Kommission in Fragen des Datenschutzes. Die Working Paper der WP 29 sind abrufbar über die Webseiten der Europäischen Kommission

[6] Working Paper 243, Seite 12

[7] D.h. volle Anwendbarkeit der Artikel 37 bis 39 DS-GVO / Working Paper 243, Seite 5

[8] Vergleiche Artikel 37 Abs. 5 DS-GVO und § 5 Abs. 3 BDSG-NEU

[9] Working Paper 243, Seite 12

[10] Vergleiche Artikel 39 DS-GVO und § 7 BDSG-NEU

[11] Vergleiche Artikel 38 DS-GVO, §§ 6 und 7 Abs. 2 BDSG-NEU

[12] So schon die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Die Datenschutzbeauftragten in Behörde und Betrieb Info 4, Seite 18

1. ordnungsgemäße und frühzeitige Einbindung des Datenschutzbeauftragten,
2. Bereitstellung erforderlicher Ressourcen,
3. Weisungsfreiheit und Unabhängigkeit,
4. keine Benachteiligung: Abberufungs- und Kündigungsschutz,
5. unmittelbarer Berichtsweg zur höchsten Führungsebene,
6. Anrufungsrecht der Betroffenen,
7. kein Interessenkonflikt,
8. Zusammenarbeit mit der Aufsichtsbehörde.

Die Weisungsfreiheit des Datenschutzbeauftragten ist Kernstück seiner Unabhängigkeit. Sie ist nach der DS-GVO und dem BDSG-NEU beschränkt auf solche Handlungen, die sich auf die Ausübung seiner Aufgaben als Datenschutzbeauftragten beziehen.

Unternehmen und Behörden dürfen dem Datenschutzbeauftragten gegenüber somit keine Weisungen in seiner Funktion als Datenschutzbeauftragter erteilen. Deshalb sind z.B. Vorgaben zur Erreichung eines bestimmten Ziels, zur Art und Weise der Bearbeitung von Beschwerden oder zum Austausch mit Aufsichtsbehörden unzulässig.

Der deutsche Gesetzgeber hat entschieden, die Unabhängigkeit der Datenschutzbeauftragten zu verstärken. Das BDSG-NEU enthält daher die Regelung, dass Abberufungen nur in entsprechender Anwendung des § 626 BGB möglich und Kündigungen nur aus wichtigem Grund zulässig sind. Darüber hinaus ist nach dem BDSG-NEU die Kündigung des Arbeitsverhältnisses nach dem Ende der Tätigkeit als Datenschutzbeauftragter innerhalb eines Jahres nach der Abberufung unzulässig, es sei denn, die kündigende Stelle ist zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt.

Die bereits aus dem aktuellen BDSG bekannten Privilegierungen bleiben somit bestehen.

13) Sanktionen und Haftung[13]

Verstöße gegen die Bestimmungen zum Datenschutzbeauftragten können zukünftig mit Geldbußen von bis zu 10.000.000 € oder im Falle eines Unternehmens bis zu 2 % seines gesamten weltweit erzielten Vorjahresumsatzes verhängt werden, je nachdem, welcher Betrag höher ist.

Vergleicht man die Regelung des Artikels 83 DS-GVO mit den aktuell anzuwendenden Bußgeldtatbeständen des BDSG, so zeigt sich, dass sich mit der Neuregelung eine erhebliche Sanktionsverschärfung für Verantwortliche und Auftragsverarbeiter ergibt.

Aufgrund des zukünftigen Aufgabenkatalogs, der die Kontroll-, Hinweis- und Beratungspflichten der Datenschutzbeauftragten deutlich erweitert, wurde in den vergangenen Monaten vermehrt diskutiert, ob hiermit auch eine weitergehende Haftung und Verantwortlichkeit des Datenschutzbeauftragen einhergeht.

Die WP 29 hat sich hierzu bereits positioniert und führt aus, dass Überwachung der Einhaltung der gesetzlichen Bestimmungen nicht bedeute, dass der Datenschutzbeauftragte auch persönlich verantwortlich sei, wenn ein Verstoß gegen datenschutzrechtliche Bestimmungen festgestellt werde. Die Einhaltung des Datenschutzes sei die unternehmerische Pflicht des Verantwortlichen/Auftragsverarbeiters und nicht des Datenschutzbeauftragten.[14]

Die DS-GVO verlagert somit die Pflicht zur Einhaltung datenschutzrechtlicher Regelungen nicht einseitig auf die behördlichen und betrieblichen Datenschutzbeauftragten – vielmehr werden Verantwortlichem und Auftragsverarbeiter explizit Aufgaben zugewiesen, durch die der Datenschutzbeauftragte in die Lage versetzt werden soll, seine Aufgaben zu erfüllen.

Verantwortlich bleibt daher in erster Linie der Verantwortliche oder Auftragsverarbeiter.

Unabhängig von der Frage der Umsetzungsverantwortung obliegt dem Datenschutzbeauftragten gleichwohl die Erfüllung der in der DS-GVO und dem BDSG-NEU genannten Aufgaben, sodass unter Umständen auch eine persönliche Haftung des Datenschutzbeauftragten in Betracht kommen kann.

[13] Vergleiche Artikel 83 Abs. 4 lit. a DS-GVO

[14] Working Paper 243, Seite 24/25

Es wird daher dringend dazu angeraten, dass der Datenschutzbeauftragte eigenständig Beratungs- und Überwachungsmaßnahmen dokumentiert, um nachweisen zu können, dass er die ihm obliegenden Aufgaben ordnungsgemäß erfüllt.

Fazit:

Ob es die Pflicht zur Benennung, die persönlichen Voraussetzungen des Datenschutzbeauftragten, seine Aufgaben und Pflichten oder seine Stellung betrifft – die in Artikel 37 bis 39 DS-GVO enthaltenen Regelungen sowie die ergänzenden Regelungen des BDSG-NEU erfinden die Rechtsfigur des Datenschutzbeauftragten nicht neu, sondern knüpfen an bereits bekannte und bewährte Regelungen an.

Gleichwohl empfiehlt sich vor dem Hintergrund der im Detail neuen Regelungen, der Erweiterung des Aufgabenkatalogs sowie der erheblichen Haftungsverschärfung eine intensive und kritische Auseinandersetzung mit den neuen gesetzlichen Bestimmungen. Auf diese Weise kann Handlungsbedarf erkannt und gegebenenfalls nachgebessert werden.

Die Handreichung des Hessischen Datenschutzbeauftragten „Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht“ soll Verantwortlichen, Auftragsverarbeitern und Datenschutzbeauftragten hierbei eine hilfreiche Unterstützung sein.

Über die Autorinnen:

Yvonne Herzog & Katja Horlbeck
Der Hessische Datenschutzbeauftragte

▶ https://www.datenschutz.hessen.de

https://www.datenschutz.hessen.de/download.php?download_ID=373&download_now=1

DER HESSISCHE DATENSCHUTZBEAUFTRAGTE

ZERTIFZIERUNG – EIN ZWISCHENSTAND

Dr. Niels Lepperhoff

Mit der DS-GVO nimmt der Gesetzgeber einen neuen Anlauf Zertifizierung im Datenschutzrecht zu verankern. Zertifikate können helfen, die Einhaltung verschiedene Vorschriften der DS-GVO nachzuweisen. Um diese Wirkung entfalten zu können, bedarf es einer Akkreditierung und Genehmigung durch Datenschutzaufsichtsbehörde. Mit dem BDSG-Neu hat der deutsche Gesetzgeber einen zweistufigen Akkreditierungsprozess etabliert. Eine Zertifizierungsstelle benötigt eine Akkreditierung bei der Deutsche Akkreditierungsstelle GmbH (DAkks). Dabei müssen neben den allgemeinen Kriterien auch weitere Vorgaben der deutschen Datenschutzaufsichtsbehörden erfüllt werden. Diese Vorgaben befinden sich aktuell in einer Abstimmung zwischen den Aufsichtsbehörden. An eine erteilte Akkreditierung schließt sich die Zulassung durch die zuständige Datenschutzaufsichtsbehörde an. Diese prüft dann den der Zertifizierung zugrundliegenden Standard.

Da die deutschen Datenschutzaufsichtsbehörden ihre Akkreditierungskriterien noch nicht verabschiedet haben, lässt sich aktuell weder ein Antrag stellen noch absehen, welche Anforderung im Detail gestellt werden.

Die DSZ Datenschutz Zertifizierungsgesellschaft mbH (DSZ) steht in engen Kontakt mit der LDI NRW um eine Akkreditierung und Zulassung vorzubereiten. Grundlage soll eine überarbeitete Version des Standards DS-BvD-GDD-01 sein. In einer Arbeitsgruppe von BvD und GDD wurde der Standard an die Vorgaben der DS-GVO angepasst. Die grundlegende Struktur wurde beibehalten und um neue Anforderungen der DS-GVO ergänzt. Bspw. wurden die Betroffenenrechte erweitert. Auf der anderen Seite sind Regelungen entfallen, wenn diese im Lichte der DS-GVO entbehrlich geworden sind. Das Kapitel zum Sicherheitskonzept wurde deutlich entschlackt. Mit dieser überarbeitenden Version gehen wir in die Gespräche mit dem LDI NRW. Bis zum Abschluss der Gespräche ist der Standard vorläufig und kann deshalb nicht veröffentlich werden.

Über den Autor

Dr. Niels Lepperhoff
Geschäftsführer DSZ Datenschutz Zertifizierungsgesellschaft mbH

DSZ DATENSCHUTZ Zertifizierungsgesellschaft n
EIN UNTERNEHMEN VON GDD UND BVD

AUS DEM VERBAND

GUTACHTEN DES BVD ZU STELLUNG, PFLICHTEN UND HAFTUNG DES DSB IN DER DS-GVO

Konrad Menz

Die zum 25.05.2016 in Kraft getretene und ab dem 25.05.2018 unmittelbar anzuwendende Datenschutz-Grundverordnung führt im Hinblick auf die Stellung des Datenschutzbeauftragten zu einer rechtlichen Unsicherheit, die über die reinen Fragen der Änderungen im Datenschutzrecht hinaus auch Fragen des Arbeitsrechts, Zivilrechts und des Strafrechts betrifft.

Um der festzustellenden Rechtsunsicherheit begegnen zu können, hat der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. die Einholung einer gutachterlichen Stellungnahme zu den Änderungen der Stellung des Datenschutzbeauftragten durch die Datenschutz-Grundverordnung veranlasst. Die entsprechende Ausarbeitung wurde am 26.10.2017 im Rahmen der BvD-Herbstkonferenz Datenschutz in Stuttgart präsentiert. Die wichtigsten Erkenntnisse werden nachstehend kurz zusammengefasst.

Der unter Geltung des aktuellen Bundesdatenschutzgesetzes bestellte Datenschutzbeauftragte bleibt auch nach Wirksamwerden der Datenschutz-Grundverordnung grundsätzlich im Amt. Die Bestellungen bleiben als Benennungen wirksam, jedoch gilt ab dem 25.05.2018 unmittelbar die Datenschutz-Grundverordnung.

Arbeitsverträge der internen Datenschutzbeauftragten enden nicht automatisch mit dem Anwendungsbeginn der Datenschutz-Grundverordnung. Jedoch sind die Voraussetzungen der Pflichtbestellung, des Kündigungsschutzes sowie des Schutzes gegen Abberufung und Benachteiligung in der Datenschutz-Grundverordnung anders als in dem bis zum Ablauf des 24.05.2018 geltenden Bundesdatenschutzgesetz geregelt. Der deutsche Gesetzgeber hat aber zwischenzeitlich mit einem zum 25.05.2018 in Kraft tretenden neuen Bundesdatenschutzgesetz (namensgleich, nachfolgend BDSG-neu genannt) dafür gesorgt, dass die bisherigen Regelungen zum Kündigungsschutz und zur Pflichtbestellung weitgehend in einer an die Datenschutz-Grundverordnung angepassten Form erhalten bleiben.

Für den externen Datenschutzbeauftragten gilt, dass weder die Bestellung noch seine Beauftragung mit dem Anwendungsbeginn der Datenschutz-Grundverordnung automatisch enden. Er haftet auch nicht für jeden Datenschutzverstoß, kann sich aber auf eine Haftungsprivilegierung, wie sie dem internen Datenschutzbeauftragten zuteil wird, nicht berufen.

Auch die Rolle des Datenschutzbeauftragten erfährt durch die Datenschutz-Grundverordnung eine Änderung. Von besonderem Interesse ist hier sicherlich, inwieweit die dem Datenschutzbeauftragten nach Artikel 39 Abs. 1 lit.b DS-GVO zugewiesene Aufgabe der „Überwachung der Einhaltung dieser Verordnung“ für ihn haftungs- und sanktionsrechtliche Risiken birgt. Für ein zutreffendes Verständnis des Begriffs der „Überwachung“ sind jedoch nicht nur isoliert die Terminologie, sondern auch das allgemein durch die Datenschutz-Grundverordnung begründete Rollenverständnis zwischen dem Verantwortlichen (in der Regel die Unternehmensleitung) und dem Datenschutzbeauftragten mit einzubeziehen. Danach ist festzustellen, dass im Mittelpunkt der datenschutzrechtlichen Pflichten der Verantwortliche steht. Der Datenschutzbeauftragte selbst überwacht lediglich die datenschutzrechtliche Organisationsstruktur des Unternehmens und berichtet über seine insoweit gewonnenen Erkenntnisse gegenüber dem obersten Management. Die Intensität seiner Berichterstattung hat der Datenschutzbeauftragte hierbei an dem risikobasierten Ansatz, von dem die Datenschutz-Grundverordnung auch insoweit geprägt ist (Art. 39 Abs. 2 DS-GVO), auszurichten. Sein durch die Datenschutz-Grundverordnung vorgegebener Pflichtenkreis umfasst hingegen in Ermangelung entsprechender Weisungsbefugnisse keine Pflicht zum aktiven Eingreifen, um einzelne Verstöße zu beseitigen oder zu verhindern.

Aus der Datenschutz-Grundverordnung ergibt sich auch keine unmittelbare sanktionsrechtliche Verantwortlichkeit des Datenschutzbeauftragten, etwa als Adressat eines Bußgeldes. Art. 83 DS-GVO richtet sich nur gegen den Verantwortlichen und den Auftragsverarbeiter. Anders als für den Compliance-Officer ergibt sich ein sanktionsrechtliches Risiko für den Datenschutzbeauftragten auch nicht aus einer Garantenstellung (sanktionierte Untätigkeit, weil man hätte handeln müssen), sofern sich seine Aufgaben an den originären Vorgaben der Datenschutz-Grundverordnung ausrichten. Ist der Datenschutzbeauftragte hingegen bereit, im Wege der Delegation erweiterte Pflichten und Befugnisse zu übernehmen, so kann sich hieraus eine Garantenstellung mit der Folge ergeben, dass auch der Datenschutzbeauftragte eine sanktionsrechtliche Ahndung befürchten muss. Zudem ist bei der Delegation zu gewährleisten, dass die zusätzlichen Aufgaben nicht zu einem Interessenkonflikt mit den originären Aufgaben des Datenschutzbeauftragten aus der Datenschutz-Grundverordnung führen. In jedem Falle ist zur Vermeidung von Unklarheiten dringend anzuraten, die Delegation vertraglich zu regeln und für die erweiterten Aufgaben eine Deckungszusage der Versicherung einzuholen.

Auf den für die Praxis äußerst relevanten Spannungsbogen zwischen der Delegation zusätzlicher Aufgaben und Befugnisse einerseits und andererseits den originären Aufgaben des Datenschutzbeauftragten wurde in der gutachterlichen Stellungnahme nicht näher eingegangen, da dies nicht von dem erteilten Auftrag umfasst war. Dieser Thematik – auch unter Würdigung des Art. 38 Abs. 6 DS-GVO – wird bis zum 25.05.2018 noch im Detail an anderer Stelle nachzugehen sein.

Gleichwohl stellt die gutachterliche Stellungnahme einen wichtigen Baustein für die Klärung grundlegender Fragen und die Einordnung von Risiken und Veränderungen dar, wie sie sich mit dem Anwendungsbeginn der Datenschutz-Grundverordnung ergeben werden.

Die Studie kann unter www.bvdnet.de abgerufen werden.

Über den Autor

Konrad Menz

Rechtsanwalt und Partner der überregional tätigen Wirtschaftskanzlei Derra, Meyer & Partner am Standort Ulm, verfügt über eine langjährige Erfahrung im Bereich des Wirtschaftsstrafrechts sowie in Bußgeldverfahren gegen Wirtschaftsunternehmen und berät zudem präventiv zu Fragen der Compliance. Regelmäßige Referententätigkeit zum Sanktionsrecht nach der Datenschutz-Grundverordnung.

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

SCHULUNGSKONZEPT DES AK ARBEITSHILFEN

Regina Mühlich/Prof. Bernd Beier

Die Mitglieder des AK Arbeitshilfen erarbeiten Vorlagen, Checklisten, Konzepte etc. um bei den Aufgaben des Datenschutzbeauftragten zu unterstützen und zu erleichtern. Mit der Einführung der DS-GVO tut sich ein breites Feld auf. Viele Prozesse und Dokumente müssen angepasst, überarbeitet und neu erstellt werden. Für die Themen, die den DSB besonders betreffen, wurde ein Arbeitskreis installiert, der sich dieser wichtigen Aufgabe widmet. Zu allererst hat sich der Arbeitskreis den geänderten Anforderungen an die „Schulungsmaßnahmen" gestellt.

Die einheitliche EU-Regelung des Datenschutzrechts mit der DS-GVO hat auch Auswirkungen auf die zukünftige Gestaltung der anzusetzenden und entsprechend vorzubereitenden Maßnahmen betreffender Unterweisungen und Schulungen zum Datenschutz. Mit dem Gültig werden der DS-GVO zum 25. Mai 2018 sind daher die Anforderungen an die in Zukunft vorzunehmenden Unterrichtungs-Maßnahmen in den verantwortlichen Stellen neu aufzustellen. Die zu ergreifenden Schulungsmaßnahmen müssen dabei in ein entsprechendes „Datenschutzmanagement" eingebettet sein.

Beim Datenschutzmanagement geht es darum, durch unternehmensleitende Maßnahmen den Anforderungen des Datenschutzes gerecht zu werden. Dabei spielt der Datenschutzbeauftragte eine zentrale Rolle. Er ist Bestandteil eines umfassenden Managements, bei dem weitere Rollen Bedeutung haben: die Anwender, die IT-Abteilung mit der Systemadministration, in der Regel weitere Abteilungen, insbesondere die zuständig sind für Personal, für die Finanzen, für den Umgang mit den Kundendaten (Marketing). Diesbezüglich müssen daher auch die zu planenden Schulungsmaßnahmen mit im Vordergrund stehen. Je nach Art des organisatorischen Zusammenhangs sind weiterhin die jeweiligen Schnittstellen innen wie nach außen von großer Bedeutung.

Hier müssen auch die jeweiligen Planungen für die einzelnen Schulungslevels überdacht und konkretisiert werden.

Zum einen ist zunächst eine „einfache Unterweisungen" zu entwerfen, als allgemeinen Überblick für die unterste Ebene der Vermittlung von Datenschutz-Kenntnissen. Daneben bzw. darüber hinaus und dann jeweils aufeinander aufbauend sollten Schulungsmaßnahmen entworfen werden, die dann im klassischen Seminarunterricht, aber auch unterstützend in digitaler Form zu erarbeiten sind.

Hierzu soll das vom AK Arbeitshilfen entwickelte Schulungs-Schema mit der Einbeziehung der jeweiligen Personengruppen (Level I bis III) eine Hilfestellung bieten. Das Schema ist natürlich variabel zu sehen und ggf. auch - in entsprechenden Sonderfällen - zu erweitern, z.B. spezielle „Schulungs"maßnahmen für Vorstände, Geschäftsführung, Stabstellen und Betriebsräte.

Die Aufteilung in den vorgeschlagenen drei Levels sind daher als ein erster Ansatz zu verstehen, der natürlich jeweils auch nach den eigenen Erfahrungen des DSB in der jeweiligen Situation des Unternehmens zu bewerten ist.

Schulungsmaßnahmen sind nicht als Einzelaktion zu sehen, sondern eingebettet in ein Gesamtkonzept des Unternehmens von Unterweisungen und Schulungen.

Zu beachten ist auch die korrekte Dokumentation der Veranstaltungen mit Inhalten, sei es elektronisch, Papierform, immer an die Nachweispflicht denken, etc.

Die konkretisierte Einbindung der einzelnen Aufgabengebiete bzw. Fachbereiche und Zuordnungen sollten aufgeteilt bzw. beschrieben werden können.

Alle Inforamtionen zum Schulungskonzept des AK Arbeitshilfen finden Sie auf unserer Website unter:

https://www.bvdnet.de/bvd-arbeitskreise/arbeitskreis-arbeitshilfen/

Über die Autoren

Regina Mühlich
Sprecherin des AK Arbeitshilfen

Prof. Bernd Beier
Mitglied AK Arbeitshilfen

„DATENSCHUTZ GEHT ZUR SCHULE" IM KAISERBAHNHOF

AK Schule & Initiative „Datenschutz geht zur Schule"
Ralf Heimburger

Was hätte wohl der letzte deutsche Kaiser dazu gesagt, dass sich Kapazitäten aus dem ganzen Land in seinem Bahnhof treffen um darüber zu beratschlagen, wie man Geheimnisse schützt und wie es wohl möglich wäre, Nachrichten vertraulich zu überbringen.

Tatsächlich trafen sich ca. 35 Dozenten und Gäste der Initiative „Datenschutz geht zur Schule" am 17.10.2017 in Potsdam. Der Kaiserbahnhof, welcher der königlichen Familie und Kaiser Wilhelm II. nach seiner Erbauung im Jahr 1909 als Privatbahnhof diente, war der historische Rahmen für den diesjährigen Dozententag. Die Initiative „Datenschutz geht zur Schule" (DSgzS) hat in diesem Jahr zum vierten Mal (wieder unterstützt durch die DATEV Stiftung Zukunft) ihre Dozenten eingeladen um deren ehrenamtliche Tätigkeit zu unterstützen und zu würdigen. Die Veranstaltung bietet neben Fachvorträgen auch die Plattform für die Teilnehmer um sich auszutauschen und zu netzwerken.

Gastgeber in diesem Jahr war die Deutsche Bahn AG (DB), genauer gesagt die DB-Akademie für Führungskräfte, welche ihren Sitz im Kaiserbahnhof hat. Nach einer kurzen Begrüßung der Teilnehmer durch Rudi Kramer und Frank Spaeing gab Shirish Pandit als Leiter der DB-Akademie einen Einblick in die Aufgaben und Angebote der DB-Akademie im DB-Konzern. Über Aufgaben und Hintergründe zum Datenschutz bei der DB informierte Chris Newiger in ihrer Funktion als Konzerndatenschutzbeauftragte der DB. Wie man den Datenschutz in einer Konzernstruktur organisiert und Herausforderungen in diesem Kontext meistert, erfuhren die Teilnehmer von Frau Newiger aus erster Hand.

„Spiele Apps für Kinder" war das Thema des Vortrages von Danielle Leven von der Stiftung Warentest. Interessant hierbei war zu erfahren, wie die Stiftung Warentest bei der Untersuchung und Bewertung von Produkten vorgeht.

Frau Leven erläuterte die Testkriterien, wobei die datenschutzfreundliche Umsetzung bei der Bewertung der Apps eine wesentliche Rolle spielte. Das nur wenige Apps diese Kriterien erfüllten, verwunderte die Anwesenden nicht.

Im nächsten Vortrag „Medienscouts MV machen Schule" stellte Antje Kaiser als Vertreterin des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern das Konzept der Medienscouts vor. Schüler auszubilden und zu coachen, die sich dann in ihren Schulen engagieren, wird als erfolgsversprechendes Konzept gesehen um schnell viele Schüler zu erreichen

Stefan Mairose, Leiter Audit und Technischer Datenschutz bei der DB, vermittelte den Teil-

nehmern anhand einiger Beispiele einen Eindruck darüber, welche Aspekte bei der Konzeption und Entwicklung von Lösungen und Dienstleistungen der DB im Kontext Datenschutz und Informationssicherheit eine Rolle spielen. „Alexa, buche mir eine Fahrkarte……“ war eines der Beispiele.

Die Umsetzung der DS-GVO im DB-Konzern war Thema des Vortrages von Karen Sokoll. Mit einer Gegenüberstellung von BDSG und DS-GVO hat Frau Sokoll für die anwesenden Dozenten eindrücklich aufgezeigt, in welchen Bereichen sich durch Änderungen Handlungsbedarf ergibt.

Nach der Mittagspause fand ein geführter Rundgang durch den beeindruckend restaurierten Kaiserbahnhof für die Teilnehmer des Dozententages statt. Beim Betreten der Gleishalle mit den Original-Waggons aus der Kaiserzeit konnte man sich für einen kurzen Moment vorstellen, wie hier vor 100 Jahren die Dampflock qualmte.

Spielerisch ging es danach weiter. Reinhard Muth und Susanna Wolf von der DATEV eG stellten ein selbst entwickeltes Brettspiel vor. Das Spiel wurde mit dem Hintergrund entwickelt spielerisch Wissen aus den Bereichen „Datenschutz, Informationssicherheit und Compliance“ zu vermitteln. Nachdem das Spiel vorgestellt und die Regeln erklärt waren, durften alle Teilnehmer in Gruppen selbst Hand anlegen. Es dauerte nicht lange, dann rollten die Würfel und alle waren vom Spielfieber erfasst. Ein gelungenes Spiel konnte den Referenten in ihren Feedback Bögen bescheinigt werden.

Über verschiedene Bildungsprojekte informierte Nadine Berneis von DSiN e.V.

DsiN e.V. ist ein Verbund von engagierten Unternehmen und Organisationen, die Schutz, Sicherheit und Vertrauen als Kernaufgabe in der Digitalisierung betrachten. Frau Berneis stellte u.a. das Projekt „BOTTOM-UP“ vor. Hierbei war die Fülle an Schulungsmaterial für die Dozenten interessant.

Parallelen zum Sensibilisierungskonzept von DSgzS konnten die Dozenten beim Konzept über die „Vermittlung von Datenschutzsensibilisierungen bei Grundschulen im Saarland“ erkennen. Jörg Zarth als Vertreter des Unabhängigen Datenschutzzentrums Saarland stellte sein Konzept zur Sensibilisierung von Grundschülern im Saarland vor. Hier zeigte sich, dass es interessante Anknüpfungspunkte für einen weiteren Austausch gibt.

Die durchweg sehr interessanten und informativen Beiträge, die professionelle Organisation und Betreuung sowie die exzellente Tagungsstätte haben sicher dazu beigetragen die Spannung und Aufmerksamkeit bis zum Ende des Dozententages hoch zu halten. Für die Teilnehmer des vierten Dozententages der Initiative DSgzS war es wieder mal eine lohnende Veranstaltung – so das Feedback aus abschließenden Gesprächen und Diskussionen.

Für nächstes Jahr gibt es bereits Überlegungen, so dass davon ausgegangen werden kann, dass 2018 wieder ein Dozententag stattfinden wird.

Am Vortag des Dozententages hat die Initiative DSgzS einen Aktionstag an der Leonardo-da-Vinci Gesamtschule in Potsdam durchgeführt. 11 Dozenten und Gasthörer haben so am Montag, den 16.10.2017, alle anwesenden Klassen (ca. 650 Schüler) sensibilisiert. Eine Führung durch das Neue Palais im Park Sanssouci in Potsdam für die Dozenten und ein von der Initiative DSgzS organisiertes Abendessen (der Dozentenstammtisch) rundeten den Aktionstag ab.

Über den Autor

Ralf Heimburger

Mitglied im Arbeitskreis Schule,
Dozent und Mentor der Initiative DSgzS

▶ dsgzs@bvdnet.de

Datenschutz geht zur Schule
BvD e.V.
DATENSCHUTZ GESTALTEN

NEUE RUNDE BEIM NÜRNBERGER DATEN-DIENSTAG

Mit Unterstützung des BvD setzt das Museum für Kommunikation in Nürnberg seine Reihe „Daten-Dienstag“ mit Veranstaltungen zu Themen rund um den Datenschutz fort. Nach dem Screening des Kinofilms „The Circle“ als Special stehen unter anderem die Themen Menschenrechte in der digitalen Welt und Gesundheitsprogramme von Versicherungen auf der Agenda.

Am 23. Januar ist der Nürnberger Kriminalhauptkommissar Stefan Malek zu Gast. Er spricht über Formen der Radikalisierung im Internet. Zum Safer Internet Day am 06. Februar 2018 referiert der Leiter des Career Service der Hochschule Aschaffenburg Ernst Schulten zum Thema „Tracking im Web 3.0.“

Im März diskutiert Andreas Sachs vom Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) mit den Gästen über Datenkraken und Cyperdiebe.

Zur Nürnberger Web Week im April 2018 geht es um Trends und Tendenzen in der Marktforschung. Redner ist Roland Abold von der GfK, die auch die Einschaltquoten für Deutschland erhebt.

Die frühere Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) beendet die Reihe am 12. Juni 2018 mit einem Vortrag über die Europäischen Grundrechte und deren Bedeutung für die informationelle Selbstbestimmung im digitalen Zeitalter.

Der BvD initiierte und unterstützt die Reihe seit ihrem Start 2015, neuer Kooperationspartner ist das BayLDA. Die Veranstaltungen beginnen jeweils um 19 Uhr, der Eintritt ist frei.

Daten-Dienstag Privatheit im Netz

Beginn 19 Uhr
Museum für Kommunikation Nürnberg
Eintritt frei

Der digitale Wandel ist in vollem Gange und durchdringt mit Smartphone und Tablet unseren Alltag. Daher lohnt es sich, namhafte Fachleute zum überlegten Umgang im Netz zu hören und mit ihnen ins Gespräch zu kommen.

26.09.2017 **Payback: Wie geht Kundenbindung?**
André Pallinger, Mitglied der Geschäftsleitung, PAYBACK GmbH

24.10.2017 **Menschenrechte in der digitalen Welt**
Ing. Mag. Dr. Christof Tschohl, Research Institute AG & Co KG – Zentrum für digitale Menschenrechte, Wien

21.11.2017 **Generali Vitality – Ein Gesundheitsprogramm als Zukunftsmodell für Versicherungen**
Astrid Koida, Head of Vitality Deutschland, München

23.01.2018 **Formen der Radikalisierung im Internet**
Stefan Malek, Kriminalhauptkommissar, Kommissariat 34 Nürnberg

06.02.2018 Safer Internet Day 2018
Ich weiß, was Du morgen getan hast – Tracking im Web 3.0
Ernst Schulten, social-media-webhygiene, Aschaffenburg

20.03.2018 **Von Datenkraken, Schlapphüten und Cyberdieben – Datenschutz im Netz?**
Andreas Sachs, Dipl.-Inf. (Univ.), Vertreter des Präsidenten, BayLDA, Ansbach

17.04.2018 Nuernberg Web Week
Wie funktioniert Marktforschung heute?
Dr. Roland Abold, Gfk, Nürnberg

12.06.2018 **Europäische Grundrechte als Garant für die informationelle Selbstbestimmung im digitalen Zeitalter?**
Sabine Leutheusser-Schnarrenberger, Bundesjustizministerin a.D.

Eine Kooperation des Museums für Kommunikation mit dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) und dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Verkehrsverbindungen
U2, U3 Haltestelle Opernhaus

Museum für Kommunikation Nürnberg
Lessingstraße 6, 90443 Nürnberg
Tel. +49 (0)911 230 88-0
mfk-nuernberg@mspt.de, www.mfk-nuernberg.de

Ein Museum der Museumsstiftung Post und Telekommunikation
Getragen von der Deutschen Post und der Deutschen Telekom

Bayerisches Landesamt für Datenschutzaufsicht

BVD BEFRAGT UNTERNEHMEN ZUM START DER DS-GVO IM MAI 2018

Der BvD wird zum Start der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018 Unternehmen zum Stand der Vorbereitungen befragen. BvD-Vorstand Thomas Spaeing befürchtet, dass viele Betriebe ihre Datenschutz-Systeme noch nicht rechtzeitig auf die neuen Anforderungen umstellen werden.

> *„Dann drohen ihnen saftige Geldstrafen", sagt er. „Wir wollen herausfinden, wie weit die Unternehmen die Anforderungen an die neuen Regelungen erfüllen und ob sie noch Unterstützung von unseren Experten benötigen."*

Eine Umfrage des Digitalverbands Bitkom unter rund 500 Datenschutz-Verantwortlichen in Betrieben ab 20 Mitarbeitern fand jüngst heraus, dass bislang nur drei Prozent der Befragten mehr als die Hälfte der notwendigen Vorbereitungen erfüllt haben. Fast jedes zweite Unternehmen (47 Prozent) hat bis jetzt nur zehn Prozent oder gar keine Aufgaben in Angriff genommen. Nur 15 Prozent glauben, dass sie zum 25. Mai die Verordnung vollständig umsetzen werden, jedes zweite Unternehmen (54 Prozent) denkt, dass es das nur teilweise schafft.

Als Gründe für die schleppende Vorbereitung führen die Verantwortlichen laut Bitkom einen schwer abschätzbaren Umsetzungsaufwand, Rechtsunsicherheit und einen Mangel an praktischen Umsetzungshilfen an. 30 Prozent sind der Auffassung, dass der zweijährige Umsetzungszeitraum zu kurz sei. Sie wünschen sich finanzielle Unterstützungen etwa durch Förderprogramme, Auslegungshilfen und längere Übergangsfristen.

Der BvD bietet unter anderem mit Informationsveranstaltungen Praxisleitfäden und Stellungnahmen umfangreiche Unterstützung für Firmen zum Start der DS-GVO an. Zudem beraten die Verbandsmitglieder Unternehmen bei der Umsetzung.

Weitere Informationen finden Interessierte auf

www.bvdnet.de.

RECHTSHANDBUCH INDUSTRIE 4.0 UND INTERNET OF THINGS

Sassenberg / Faber

Sassenberg / Faber
»Rechtshandbuch Industrie 4.0 und Internet of Things«
C.H.BECK
2017. Buch. XXIV, 538 S.:
mit Abbildungen. Hardcover (In Leinen)
ISBN 978-3-406-70869-5

Das Buch kommt nicht nur in neuer optischer Aufmachung als Teil einer neuen Reihe des Verlags, sondern behandelt wohl erstmalig die unterschiedlichen Bereiche von Industrie 4.0 und IoT in dieser Komplexität. Auch wenn sich das Buch als Rechtshandbuch im Wesentlichen an Juristen wendet, bearbeitet es die vielen Facetten eines komplexen Themas und trägt dabei den unterschiedlichsten Bereichen von Maschinenbau, Produktion, der Automobilbranche über Medizin und Gesundheit, Gebäude- und Sicherheitstechnik, elektronischen Bezahlsystemen bis zu Verkaufsautomaten - um nur einige zu nennen - Rechnung.

Ein großer Teil des Buches wird dem Thema Datenschutz und IT-Sicherheit gewidmet. Innerhalb der einzelnen Kapitel wird im Rahmen der unterschiedlichen Betrachtungen über Vertragsabschlüsse beim Rechtsgeschäft, Informationspflichten bei Verbraucherverträgen oder der Sammlung von Gesundheitsdaten immer wieder auf Datenschutz-Themen eingegangen. An einigen Stellen finden sich im Buch Checklisten, an vielen Stellen so genannte Praxis-Tipps, die drucktechnisch gesondert hervorgehoben sind.

Das Werk umfasst fünf Teile. Eine Einführung in den Weg von Industrie 4.0 zum Verständnis. Einen allgemeinen, rechtlichen Teil. In diesem Teil werden die Anforderung des Telekommunikationsrechts, des Datenschutzes und der IT-Sicherheit behandelt. Der dritte Teil widmet sich den Besonderheiten bei Vertragsabschlüssen und deren Gestaltung während sich der vierte Teil mit den Besonderheiten ausgewählter Branchen beschäftigt. Teil fünf gibt einen Ausblick auf europäische und amerikanische Perspektiven.

In der Einführung stellen die Autoren den Weg von Industrie 4.0 und IoT anschaulich dar. Im Kapitel der besonders ausgewählten Branchen von eHealth, Automotive bis zur Digitalisierung in der Bankenwelt werden in den rechtlichen Aspekten auch immer die Bereiche des Datenschutzes berücksichtigt. Das Buch ist unbedingt empfehlenswert. Es stellt die unterschiedlichen Facetten eines komplexen Themas, auch für Nichtjuristen, anschaulich und verständlich dar.

Rezension von
Jürgen Hartz
Stellv. Vorstandsvorsitzender des BvD

BvD e.V.
DATENSCHUTZ GESTALTEN

LEITFADEN ZUR DATENSCHUTZ-GRUNDVERORDNUNG

Lepperhoff, Dr. Niels / Müthlein, Thomas

Lepperhoff, Dr. Niels / Müthlein, Thomas
»Leitfaden zur Datenschutz-Grundverordnung«

Datakontext GmbH

1. Aufl. 2017
ISBN-978-3-89577-793-6
44,99 Euro

Das Werk ist ein Leitfaden von Praktikern für Praktiker – weder beschränkt auf den Datenschützer mit technischem Hintergrund noch beschränkt auf den Datenschützer mit juristischem Hintergrund. Denn beide Autoren sind seit vielen Jahren als Praktiker und Datenschutzbeauftragte tätig und haben einerseits einen technischen und andererseits einen juristischen Hintergrund.

Deutlicher als der Untertitel des Werkes die Zusammenstellung des Inhalts aufzeigt kann die Beschreibung des Inhalts kaum erfolgen: Detailfragen und erste Schritte in der betrieblichen Praxis. Es geht also auch um das Warum, aber vor allem auch um das Wie!

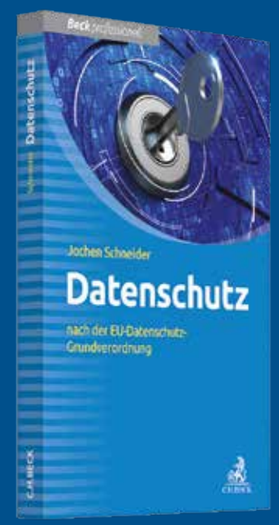
Das Werk konzentriert sich – wie die Herausgeber im Vorwort selbst ansprechen – auf die Umsetzung der DS-GVO in dem betrieblichen und behördlichen Alltag. Ausgehend von der Erfassung des Handlungsbedarfs durch die DS-GVO aus verschiedenen Perspektiven werden Ansätze zur Umsetzung der Vorgaben der DS-GVO – auch im Detail – diskutiert. Dementsprechend folgt das Werk auch nicht dem Ansatz, dem Leser die DS-GVO in der Reihenfolge deren Artikel sondern thematisch in der Struktur von Umsetzungsansätzen zu erläutern.

Den Autoren gelingt dies unterstützt durch Tabellen und Übersichten sehr gut. Neben dem Verständnis für die Anforderungen und deren Umsetzung schaffen sie aber auch die Grundlage zur Befriedigung des Erklärungsbedürfnisses, dem derzeit jeder Datenschutzbeauftragte in seinem Unternehmen ausgesetzt ist.

Ein rundum gelungenes Werk zur Unterstützung bei der Umsetzung der Vorgaben der DS-GVO!

DATENSCHUTZ NACH DER EU-DATEN-SCHUTZ-GRUNDVERORDNUNG

(Schneider, Jochen)



Schneider, Jochen
»Datenschutz nach der EU-Datenschutz-Grundverordnung«

Verlag C.H. Beck

2017, Seiten 323,
ISBN 978-3-406-70213-6,
24,90 Euro

Das Werk ist eine Einführung in die Datenschutz-Grundverordnung (DS-GVO). Aufgrund des Zeitpunkts seines Erscheinens konnte das DSAnpUG und das BDSG-neu nicht berücksichtigt werden. Auch verzichtet das Werk – wie der Autor in der Einleitung klargestellt – weitgehend auf Internetfundstellen sowie Nachweise aus Literatur- und Rechtsprechung. Das Ziel ist es den privatwirtschaftlichen Unternehmen eine fundierte Einführung zu geben.

Um eine leichte Einarbeitung zu ermöglichen, gibt das Werk an den relevanten Stellen den Text des Gesetzes wieder, sodass nicht zusätzlich noch ein Gesetzestext für das Verständnis herangezogen werden muss. Dies erleichtert dem Leser die Auseinandersetzung und das Verständnis der nicht immer leicht eingängig formulierten Regelungen der DS-GVO. Darüber hinaus werden durch Markierungen hervorgehoben Beispiele sowie Tipps, Aufzählungen und Checklisten gegeben, welche die Zugänglichkeit des Themas gerade (auch) für den/die Nichtjuristen/in als Leser/in erleichtert.

In den Kapitel 1 bis 11 werden die Regelungen der DS-GVO dargestellt und eindrücklich in ihrem Zusammenhang erklärt. Im Rahmen der Darstellung der Zulässigkeit werden neben den Regelungen der DS-GVO auch Spezialthemen der Verarbeitung personenbezogener Daten wie Direktmarketing, Profiling, Big Data, Cloud-Modelle, RFID, u.a. angesprochen. In Kapitel 12 widmet sich der Autor auf 8 Seiten der Frage „was tun". Im letzten Kapitel behandelt er die Bußgelder und Sanktionen.

Das Werk ist eine gelungene Einführung in die DS-GVO. Von einem der ganz Großen des EDV-Rechts und seit vielen Jahren Kennern des Datenschutzrechts war auch nichts anderes zu erwarten!

Rezensionen von

Dr. Jens Eckhardt
Fachanwalt für Informationstechnologierecht
Datenschutz-Auditor (TÜV)
Mitglied im Vorstand des BvD und
Compliance-Officer (TÜV)

BvD e.V.
DATENSCHUTZ GESTALTEN

BIG DATA UND E-HEALTH

Stiftung Datenschutz (Hrsg.)

Stiftung Datenschutz (Hrsg.)
»„Big Data und E-Health«

Erich Schmidt Verlag

Band 2 der Reihe Daten Debatten
1. Auflage 2017, 201 Seiten
ISBN-13: 978-3503174911
42,00 Euro

Wieder trägt die Stiftung Datenschutz mit dem zweiten Band ihrer Reihe „DatenDebatten" zur Diskussion um die Verarbeitung von personenbezogenen Daten in einem besonderen Kontext bei. Die erforderliche gesellschaftliche Diskussion zur Verwendung personenbezogener Daten außerhalb der unmittelbaren Patientenbehandlung hat bisher nur einen engen Fachkreis erreicht, obwohl die Thematik jeden betrifft oder eines Tages betreffen kann.

Die Fragestellungen umfassen hierbei mehr als nur den Einsatz von Praxisverwaltungssystemen in Arztpraxen und Krankenhäusern. Elektronische Gesundheitskarten, Videokonferenztechnik bei Ferndiagnosen, Cloud Computing und Berücksichtigung der Offenlegung von Gesundheitsdetails bei Versicherungsverträgen mit evtl. Auswirkungen auf das Solidaritätsprinzip sind nur einige der Stichworte die hierbei zu nennen sind. Die Möglichkeiten des Technikeinsatzes im Gesundheitsbereich bergen auch Risiken für den Einzelnen, die es abzuwägen und durch Maßnahmen möglichst gering zu halten gilt.

Die Autoren tragen mit unterschiedlichen Blickwinkeln auf diese Thematiken zu einem vielfältigen Kaleidoskop der Meinungen bei und regen zum Nachdenken an. Die Spannbreite der erörterten Themen ist immens: Sie umfasst den Einsatz der datenschutzkonforme eAkte, die Problematik der informierten Einwilligung, aber auch philosophische Ausführungen zur Begrifflichkeit der Optimierung. Datenschutzrechtliche Aspekte zu Big Data im Gesundheitswesen sind ebenso zu finden wie die Ausführungen zu einem App-gestützten Fitnessprogramm aus Sicht eines Krankenversicherers und die Chancen der Patientenorientierung durch die Digitalisierung durch die Brille des Verbraucherschützers. Der ehemalige BfDI Peter Schaar widmet sich dem Thema, wie viel Datenschutz ein digitales Gesundheitssystem braucht und Thilo Weichert plädiert für ein Bund-Länder-Forschungsprogramm zu den Herausforderungen der medizinischen Forschung und des Datenschutzes. Ergänzt wird dies durch Ausführungen zu Herausforderungen im Gesundheitsdatenschutz durch Wearables, eine etwas provozierende These aus Soziologensicht („Man kann Menschen nicht vor etwas schützen, wonach sie sich sehnen") bis hin zu ethischen Überlegungen zur Erhaltung der Privatsphäre im „Internet Panoptikum".

Die Beiträge sind verständlich und kurzweilig verfasst und die Zusammenstellung bietet durch die unterschiedlichen Blickwinkel einen umfassenden Eindruck über die Möglichkeiten bei gleichzeitigem Einfordern von rechtlichen Leitplanken, die zu definieren sind. Wer diese definieren müsste ist der Gesetzgeber, der dazu aber eine gesellschaftliche Diskussion und einen Konsens benötigt.

Dieser Band der „DatenDebatten" liefert eine Basis dazu. Er empfiehlt sich nicht nur für den Datenschutzbeauftragten im medizinischen Bereich, sondern auch für jeden, der bei dieser Thematik auf der Höhe der Zeit informiert sein möchte. Und nicht nur deshalb, weil er jederzeit betroffen sein könnte oder es bereits schon ist.

EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG

Gernot Syrow (Hrsg.)

Gernot Syrow (Hrsg.)
»Europäische Datenschutzgrundverordnung«
Handkommentar
Nomos Verlag
1. Auflage 2017, 1456 Seiten
ISBN-13: 978-3848717828
128,00 Euro

Es scheint fast so, als solle das Datenschutzrecht in der deutschen Rechtsliteratur das Steuerrecht von Platz 1 der Anzahl der Veröffentlichungen verdrängen. Wieder ein Kommentar, wieder in einem handlichen Format als Handkommentar gedacht und wieder mit der Darstellung der Datenschutz-Grundverordnung.

Der Herausgeber verfolgt mit diesem Handkommentar nicht nur das Ziel, die materiellen Neuregelungen im Datenschutzrecht zu interpretieren und Lösungen für die zahlreichen Anwendungsfragen des materiellen Rechts zu erarbeiten. Er möchte mit diesem Werk auch konzeptionell die Konsequenzen aus dem Rechtsformwechsel von einer Richtlinie zu einer Verordnung aufzeigen.

Der Kreis der über 20 Autorinnen und Autoren setzt sich mehrheitlich aus Hochschulangehörigen aber auch aus Praktikern wie Rechtsanwälten und bestelltem Datenschutzbeauftragtem zusammen.

Die Kommentierungen folgen einer einheitlichen Struktur, bei der zunächst die Norm und bezugnehmende Literatur vorgestellt wird, bevor die eigentliche Kommentierung beginnt. Insbesondere der Abschnitt „Kritik und Fortentwicklungsperspektive" fällt dabei positiv auffällt, auch wenn natürlich inhaltlich nicht in allen Punkten gefolgt werden kann und dieses Kapitel nicht bei allen Artikeln Verwendung findet. Die Einführung zum Kommentar bietet einen guten und klar strukturierten Überblick über die Hintergründe und Abgrenzungsfragen der DS-GVO, aber auch schon inhaltliche Zusammenfassungen.

Die Begriffsbestimmungen werden ausführlich erläutert, wobei auffällt, dass die Bearbeiter auch die damit verbundenen relevanten Artikel kommentieren, was diesbezügliche Widersprüche in der Kommentierung ausschließt.

Erwähnenswert sind beispielsweise die Ausführungen zum Cloud Computing in Art. 28, zum Löschungsanspruch bei Big-Data-Anwendungen in Art. 17 oder zur Frage der Benennungsmöglichkeit einer juristischen Person als Datenschutzbeauftragter in Art. 37. Hier werden anschaulich die jeweiligen Problematiken und mit Begründung die bevorzugte Meinung dargestellt, aber auch anderen Ansichten Raum gegeben.

Der Kommentar hinterlässt einen fundierten Eindruck, gerade wenn man neue Gedanken und Ansätze ergänzend zu den bisherigen Standardkommentierungen sucht. Wer Handlungsanweisungen mit eindeutigen Checklisten sucht, wird hier nicht fündig. Es werden aber teilweise umfassende Darstellungen auch von umstrittenen Themen geboten, die auch für vertiefte Befassungen hilfreich sind. Seine Größe und Handlichkeit unterstützt seine Praktikabilität bei Fragestellungen, die über Alltagsthemen hinausgehen. Er empfiehlt sich für alle, die sich nicht mit der erstbesten Antwort zufrieden geben wollen.

Und auch im Steuerrecht soll es ja so sein, dass durch Interpretationen erst der Rechtsrahmen gebildet wird, so dass auch dieser Handkommentar eine Bereicherung für jeden Datenschutzanwender darstellen kann.

Rezension von

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

BvD e.V.
DATENSCHUTZ GESTALTEN

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:

01.12.2017	AK Finanzdienstleistung	**06.02.2018**	AK Medizin
12.01.2018	RG Karlsruhe	**23./24.02.2018**	AK Externe
18.01.2018	RG Mitte	**01.03.2018**	RG West
31.01.2018	AK Sozial	**16.03.2018**	RG Ulm

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

Termine und Anmeldung finden Sie auf unserer Webseite:

- www.bvdnet.de

BVD-VERBANDSTAGE

25.04./26.04.2018

u. a. mit folgenden Themen:

- Umsetzung der DS-GVO in Unternehmen
- Privacy by design/by default – Anforderungskriterien aus Kundensicht
- Datenschutz-Compliance
- Beschäftigtendatenschutz
- Einwilligung

BvD-Sonderseminare & Datenschutz-Software-Forum am 25.04.2018

SAVE THE DATE

Herbstkonferenz Datenschutz 2018
Gemeinsame Veranstaltung der Aufsichtsbehörden Baden-Württemberg, Bayern und dem BvD e.V.

24./25. Oktober 2018
Herbstkonferenz mit Plenum und parallelen Workshops

26. Oktober 2018
Behördentag und öffentliche Stellen

Anzeige

BvD e.V. DATENSCHUTZ GESTALTEN

Überblick
Seminare und Workshops November 2017 / Q1 2018

Termin	Seminar/ Workshop	Ort
06.11.2017	**Die ePrivacy-Verordnung – Ergänzung zur DS-GVO**	NH Düsseldorf Nord Referentin: 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
24.01.2018	**Die Dokumentation von Verarbeitungstätigkeiten unter der DS-GVO**	ABION Hotel Berlin Referent: Lars Kripko
08.03.2018	**Die ePrivacy-Verordnung – Ergänzung zur DS-GVO**	Novotel Frankfurt City Referentin: Kristin Benedikt
09.03.2018	**Die Dokumentation von Verarbeitungstätigkeiten unter der DS-GVO**	Novotel Frankfurt City Referent: Lars Kripko
15.03.2018	**Datenschutz-Compliance nach der DS-GVO: Sicherstellung und Überwachung**	NH Düsseldorf Nord Referenten: A. Sachs & M. Gierschmann

* nur für BvD Mitglieder

Information und Anmeldung unter www.bvdnet.de

WICHTIGE KONTAKTE

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

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

Software

Es gibt Dinge, die gehen niemanden etwas an.

FOLDERFLEX GERMAN STANDARD

Mehr Sicherheit für Ihre vertraulichen Daten.

www.folderflex.de

Marketing

FÜR DEN BESTEN EINDRUCK

www.tpdigitaldruck.de

Trend Point Marketing GmbH

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

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

Datenschutz geht zur Schule BvD e.V. DATENSCHUTZ GESTALTEN

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

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

Hier könnte Ihre Anzeige stehen! Jetzt Infos anfordern unter: bvd-gs@bvdnet.de

Auditierung

DSZ DATENSCHUTZ Zertifizierungsgesellschaft mbH

EIN UNTERNEHMEN VON GDD UND BVD

Datenschutz Zertifizierung:
unabhängig – transparent – standard-basiert

www.dsz-audit.de

Anzeige

KVD® DER SERVICE-VERBAND

FACHSEQUENZ ZUR EU-DSGV
MIT DR. CHRISTOPH BAUSEWEIN UND JÜRGEN HARTZ

37. KVD Service Congress

Service 4.0 – heute und morgen

9. & 10. November 2017
Hilton Hotel Munich Airport

Spannende Keynotes, toller Special Guest, intensives Networking, aufschlussreiche Fachsequenzen: Jetzt anmelden zum 37. KVD Service Congress!

Zum 37. Mal lädt der **Kundendienst-Verband Deutschland e. V.** zum Service Congress ein. Das zweitägige Event hat sich als eines der wichtigsten Veranstaltungen für die Dienstleistung und den Service etabliert und lockt jährlich **über 400 Teilnehmer** an.

Zu den Highlights gehören unter anderem:
- eine abwechslungsreiche Ausstellung mit **Europas größter Servicemesse**
- exklusive Einblicke in die **Trends und Prognosen der KVD-Service-Studie**
- hochwertige Impulse für Ihr Business: **Fachsequenzen und Keynote-Speaker** inspirieren für mehr Erfolg in Ihrer täglichen Praxis
- Fachsequenz zum **„Datenschutz - die neue EU-DSGV in Kundendienst und Service"** mit Dr. Christoph Bausewein und Jürgen Hartz
- jede Menge Raum und Gelegenheit zu intensivem **Networking mit Kollegen, Partnern und Kunden**
- mit **Christoph Keese** ein **Special Guest**, der über das Congress-Thema hinaus wichtige Impulse einbringt

Weitere Infos & Anmeldung unter www.kvd.de.

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

Anzeige

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.kungen und aktuelle Meldungen.

Alles inklusive:

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

3 Hefte gratis

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

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

C.H.BECK