

Ausgabe 11/2018

Dezember 2018

Liebe Leserinnen und liebe Leser,

in unserer aktuellen Ausgabe möchten wir Sie wieder über einige spannende Themen im Datenschutz informieren. In dieser Ausgabe lesen Sie unter anderem über:

- gesetzliche Betreuung
- Bestandteile der Patienten-/Bewohnerakte
- Datenlöschung
- Einsatz von Faxgeräten
- Datenschutz bei der betriebsärztlichen Vorsorge
- aktuelle Urteile
- Datenschutzvorfälle

i Quelle: https://www.lidi.nrw.de/main-menu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-abdem-25_-Mai-2018/Positionsbestimmung-TMG.pdf

i Quelle: <https://www.datenschutzbeauftragter-info.de/kirchliches-datenschutzgesetz-kdg-neue-gebote-der-katholischen-kirche/>

Datenschutz-Kontakt
datenschutzbeauftragter@factpartner.de

Datenschutz Kundeninformation

Welches Gesetz hat Vorrang?

Seit dem 25.05.2018 findet die Datenschutzgrundverordnung unmittelbare Anwendung. Das bedeutet, die DSGVO

gilt als sog. Rahmengesetz, allerdings lässt sie den Gesetzgebern der EU-Mitgliedstaaten Handlungsspielraum. Beispielsweise ist in Art. 95 DSGVO geregelt, dass die Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG) und die nationalen Umsetzungen wie das Telekommunikationsgesetz (TKG) auch nach Inkrafttreten der DSGVO weiter gelten. Jedoch



ist der Abschnitt 4 des Telemediengesetzes TMG, der Regelungen zum Datenschutz beinhaltet, nicht mehr anwendbar.

Diese Vorschriften beruhen auf der Datenschutzrichtlinie 95/46/EG, die von

der DSGVO aufgehoben wurde. Hier müssen die Regelungen der DSGVO beachtet werden. Für Kirchen und religiöse Vereinigungen oder Gemeinschaften gestattet Art. 91 DSGVO

VO eigene Gesetze zum Datenschutzrecht. Aber auch hier müssen die Regelungen der DSGVO als Rechtsrahmen berücksichtigt werden. Deshalb hat die katholische Kirche das neue Kirchliche Datenschutzgesetz (KDG) und die evangelische Kirche das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) erlassen, welche am 24.05.2018 in Kraft traten.

Fazit: Deutsche Gesetze, die die DSGVO konkretisieren, ergänzen oder modifizieren sind vorrangig anzuwenden. Bei Auslegungsfragen oder Widersprüchen gilt allerdings die DSGVO.

Gesetzliche Betreuung: Selbstständige Entscheidungen von Patienten/Bewohnern

Ein gesetzlicher Betreuer übernimmt stellvertretend für den Betroffenen gewisse Rechte und Pflichten. Jedoch ist das Gericht verpflichtet die Betreuung nur für diejenigen Aufgabenkreise anzuordnen, die konkret erforderlich sind. Ein Beispiel für einen Aufgabenkreis ist die Gesundheitsvorsorge. Bei der

Gesundheitsvorsorge kommt es auf die Einwilligungsfähigkeit des Betroffenen an. Sie bezeichnet die Fähigkeit das Für und Wider einer Maßnahme der Personensorge zu erkennen, die Argumente gegeneinander abzuwägen und auf dieser Grundlage eine Entscheidung zu treffen. Solange ein Betroffener in der Lage ist, solche Ent-

scheidungen zu treffen, darf niemand anderer an seiner Stelle entscheiden!

i Quelle: <http://wegweiser-betreuung.de/betreuung/einwilligungsfahigkeit>

i Quelle: <https://www.das.de/de/rechtsportal/patientenrecht/arztspflichten/dokumentationspflicht.aspx>

i Quelle: Bremer Datenschutzaufsichtsbehörde

i Quelle: <https://www.datenschutz-guru.de/wie-lange-muss-ich-die-loschung-von-daten-von-betroffenen-nachweisen-können/>

i Quelle: <https://www.chg-meridian.com/de/explore-chg/insights-overview/Balancing-e-health--data-protection--and-data-security.html>

i Quelle: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02167.html?nn=6610630

Bestandteile der Patientenakte

Die Dokumentationspflicht, damit auch die Pflicht zur Führung einer Patientenakte, ist in § 630 f BGB geregelt. Nach Absatz 2 sind insbesondere die Anamnese, Diagnosen, Untersuchungen, Untersuchungsergebnisse, Befunde, Therapien und ihre Wirkungen, Eingriffe und ihre Wirkungen, Einwilligungen,

Aufklärungen und Arztbriefe zwingend in die Patientenakte aufzunehmen. Diese Auflistung ist allerdings nicht abschließend. Umfangreichere Behandlungsmaßnahmen oder auch komplizierte und schwierig zu dokumentierende Tatsachen müssen umso genauer und vollständiger dokumentiert werden.

Zu berücksichtigen ist auch, dass die Patientenakte bzw. Bewohnerakte freizuhalten ist von persönlichen Meinungen, Ansichten oder u.U. unwahren Inhalten, welche nicht aus fachlicher Sicht für die derzeitige und künftige Behandlung wesentlich sind.

Wie lange muss ein Unternehmen die Datenlöschung nachweisen können?

Zu diesem Thema wird gerne Art. 5 Abs. 2 DSGVO (die sog. Rechenschaftspflicht) herangezogen, wonach die Information über die Löschung für ewig gespeichert werden müsste. Auf der anderen Seite sind allerdings die Grundrechte der Unternehmen wie z. B. das Recht auf unternehmerische Freiheit des Art. 16 der Grundrechte-Charta der EU (GRCh) zu berücksichtigen. Bei der Umsetzung von

Betroffenenrechte wie das Recht auf Löschung von Daten sollte darauf abgestellt werden wie lange die Verhängung eines Bußgeldes denkbar wäre. Für Bußgelder gelten gem. § 41 BDSG die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß. Das heißt auch, dass die Verjährungsvorschriften des OWiG anzuwenden sind. Entscheidend ist dann die sog. Verfolgungsverjährung, die in

§ 31 OWiG geregelt ist. Gem. § 31 Abs. 2 Nr. 1 OWiG verjährt ein Bußgeld wegen eines Verstoßes gegen die DSGVO (oder das BDSG) in drei Jahren. Hier beginnt die Verjährungsfrist, anders als im Zivilrecht, ab Begehung der Tat. Somit ist es empfehlenswert, den Nachweis der Löschung von Daten für drei Jahre aufzubewahren.

Datenlöschung auf peripheren Geräten

Wie Schriftgut und Datenträger vernichtet werden müssen ist mittlerweile vielen bekannt. Aber was passiert mit alten IT-Geräten? Auch Output-Geräte wie Drucker, Kopierer oder Multifunktionsgeräte haben Datenträger (sog. SSD-, Hybrid- oder Flashspeicher), auf denen personenbezogene Daten

gespeichert werden. Somit gelten auch für diese Geräte die strengen Auflagen der DSGVO. Hier sollten physikalische Maßnahmen wie die mechanische, thermische oder magnetische Behandlung oder das gezielte ein- oder mehrmalige Überschreiben des entsprechenden Datenträgers ausgewählt

werden, da die einfachen Löschkommandos der jeweiligen Betriebssysteme und auch die Formatierung der entsprechenden Datenträger nicht ausreichen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert auf seiner Website ausführlich über verschiedene Lösungen.

Initiative will das Fax abschaffen

In Kliniken und Arztpraxen ist das Faxgerät immer noch im Einsatz. Dabei entspricht der Versandweg per Fax, der grundsätzlich unverschlüsselt ist, in keinsten Weise den Vorgaben zum Datenschutz. Dazu kommen noch Eigenschaften wie schlechte Qualität und Unleserlichkeit, oder Zeitverzögerung bei der Übermittlung, durch die Fehler riskiert werden. Im Spätsommer 2018 erzielte die Aktion Fax-

exploit der Forscher des Security-Unternehmens Checkpoint hohe mediale Aufmerksamkeit. Die Forscher sendeten eine präparierte Faxnachricht an ein Multifunktionsgerät, um so die Kontrolle über das Gerät zu bekommen. Dadurch hätten sie weitere Geräte im internen Firmennetzwerk angreifen oder einen Schadcode ausführen können. Mit der Simulation dieses realen Sicherheitsrisikos wollten

die Forscher die Verantwortlichen der Kliniken und Arztpraxen über den Einsatz der Technologie zum Nachdenken bringen. Kürzlich wurde eine Petition gestartet.



i Quelle: Initiative Faxendicke

Datenschutz bei der Betriebsärztlichen Vorsorge

Auch bei der arbeitsmedizinischen Vorsorge durch den Betriebsarzt gilt die ärztliche Schweigepflicht. Dennoch haben Arbeitsmediziner und Arbeitgeber Informationen auszutauschen, die in der Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV) festgelegt sind:

Gem. § 3; 4 ArbMedVV ist der Arbeitgeber zur Veranlassung der Pflichtvorsorge verpflichtet und hat eine Vorsorgekartei zu führen mit Angaben, dass, wann und aus welchen Anlässen die arbeitsmedizinische Vorsorge stattgefunden hat. Der Betriebsarzt hat dem Beschäftigten und dem

Arbeitgeber gem. § 6 ArbMedVV eine Vorsorgebescheinigung mit den o.g. Informationen auszustellen; die auch die Angabe, wann eine weitere arbeitsmedizinische Vorsorge aus ärztlicher Sicht angezeigt ist, enthält.

i Quelle: Verordnung zur arbeitsmedizinischen Vorsorge (ArbMedVV)

Datenschutzvorfall: Wenn ein „Cc“ teuer wird

Einladungen, Organisatorisches oder Geschäftliches – immer wieder, wenn E-Mails einen größeren Kreis von Personen erreichen sollen, tappen Absender in die Verteiler-Falle und tragen alle Adressaten in die Felder „An“ oder „Cc“ ein. Die Folge: Alle Empfänger können lesen, wer die Mail sonst noch bekommen hat. Das kann nicht nur unangenehm, son-

dern auch teuer werden. Jedenfalls dann, wenn so etwas im Geschäftsverkehr passiert. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat gegen die Mitarbeiterin eines Handelsunternehmens wegen eines offenen Verteilers ein Bußgeld verhängt. Die Frau hatte eine Mail mit einem kurzen Standardtext an Kunden versandt, die

Adressen aber nicht im „Bcc:“-Feld verborgen, sondern für alle sichtbar gemacht. Zehn Seiten umfasste die ausgedruckte Mail – der eigentliche Inhalt machte gerade mal eine halbe Seite aus.

i Quelle: <https://www.n-tv.de/ratgeber/Wenn-ein-Cc-teuer-wird-article10942631.html>

i Quelle: <https://www.heise.de/newsticker/meldung/DSGVO-Vers-toss-Krankenhaus-in-Portugal-soll-400-000-Euro-zahlen-4198972.html>

Daten viel zu leicht zugänglich

Speicherung der Passwörter erfolgte im Klartext

i Quelle: <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo/>

Die Nennung von Firmennamen und Marken erfolgt lediglich im redaktionellen Kontext. Ggf. bestehen Namens- und Markenrechte.

Erste substanzielle Geldstrafe nach Verstoß gegen die DSGVO

In Portugal ist die europaweit erste substanzielle Geldstrafe wegen eines Verstoßes gegen die EU-Datenschutz-Grundverordnung (DSGVO) verhängt worden. Die portugiesische Datenschutzbehörde CNPD hatte Mitte Oktober 2018 bekanntgegeben, dass das Krankenhaus Barreiro Montijo 400.000 Euro bezahlen soll, berichtet die Tageszeitung Público. Der Großteil davon ist die Strafe dafür, dass viel zu viele Personen Zugriff auf Patientendaten hatten.

Für einen anderen Verstoß wurden 100.000 Euro Strafe verhängt. Der Krankenhausbetreiber hat laut Datenschutzaufsicht „bewusst“ dafür gesorgt, dass Nutzer mit dem Profil „Techniker“ in den IT-Systemen auf Daten zugreifen konnten, die eigentlich nur für Ärzte einsehbar sein dürfen. Das sei bei einem Test ermittelt worden, in dessen Rahmen solch ein Profil mit unbegrenztem Zugang erstellt werden konnte. Darüber hinaus seien in

dem System insgesamt 985 aktive Benutzer mit einem Profil „Arzt“ registriert, obwohl 2018 lediglich 296 Ärzte eingeteilt worden seien. Das Krankenhaus habe die Diskrepanz mit temporären Profilen im Rahmen eines Dienstleistungsvertrags zu erklären versucht. Das Krankenhaus Barreiro Montijo hatte im Juli Besuch von den Datenschützern erhalten. Deren Schlussfolgerungen teilt es nicht, das Krankenhaus will deswegen vor Gericht gehen.

Erstes Bußgeld nach der DSGVO jetzt auch in Deutschland

Die Bußgeldstelle des LfDI Baden-Württemberg hat im November eine Geldbuße in Höhe von 20.000 € wegen Verstoßes gegen die vorgeschriebene Datensicherheit (Art. 32 DSGVO) gegen einen baden-württembergischen Social-Media-Anbieter verhängt. Nachdem das Unternehmen bemerkt hatte, dass durch einen Hackerangriff personenbezogene Daten (darunter Passwörter und E-Mail-Adressen) von ca. 330.000 Nutzern entwendet und veröffentlicht worden sind, wandte sich das Unternehmen mit einer Datenpannenmeldung an den LfDI. Durch die Offenlegung der Datenverarbeitungs- und Unternehmens-

strukturen sowie eigener Versäumnisse fand der LfDI heraus, dass das Unternehmen durch Speicherung der Passwörter im Klartext (d. h. unverschlüsselt und unverfremdet) wissentlich gegen seine Pflicht zur Gewährleistung der Datensicherheit bei der Verarbeitung personenbezogener Daten verstoßen hat. Bei der Bemessung der Geldbuße wurden u. a. die vorbildliche Zusammenarbeit mit dem LfDI und die finanzielle Gesamtbelastung für das Unternehmen berücksichtigt, die im sechsstelligen Euro-Bereich liegt. Dr. Stefan Brink betonte abschließend: „Als Bußgeldbehörde kommt es dem LfDI nicht darauf an,

in einen Wettbewerb um möglichst hohe Bußgelder einzutreten. Am Ende zählt die Verbesserung von Datenschutz und Datensicherheit für die betroffenen Nutzer.“

Impressum
 FAC'T GmbH
 Hohenzollernring 70
 48145 Münster

info@factpartner.de
 www.factpartner.de

Telefon 0251 935-3700
 Telefax 0251 935-4075