


Ausgabe 12/2019

April 2019

Liebe Leserinnen und liebe Leser,

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

- Verschlüsselung der E-Mailkommunikation
- Bewertung von Messengerdiensten aus Datenschutzsicht
- Datenschutz bei Spenden
- Datenschutzverstöße

 Quelle: <https://www.bvdnet.de/orientierungshilfe-gesundheitsdatenschutz/>

Datenschutz-Kontakt
 datenschutzbeauftragter@factpartner.de

1

Datenschutz Kundeninformation

Die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) ist in Kraft getreten

Zum 1. März 2019 löste die Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) die bislang geltende KDO-DVO ab und bringt eine Reihe Neuerungen mit sich:

- Aktualisierte Anforderungen an den Inhalt, die Form und die Kommunikation der Verpflichtungserklärung auf das Datenheimnis
- Anforderungen an die Festlegung und Überprüfung der technischen und organisatorischen Maßnahmen (TOMs) sowohl intern als auch beim

Auftragsverarbeiter

- Aktualisierte Regelungen zum datenschutzkonformen Einsatz von E-Mails, Kopier- und Scangeräten sowie Faxgeräten
- Anforderungen an den Umgang und die Anpassung des Verzeichnisses der Verarbeitungstätigkeiten
- Festlegung von Kriterien zur Ermittlung des Schutzbedarfs personenbezogener Daten mittels Risikoanalyse
- Regelungen zu Datenschutzklassen und deren Anforderungen an den Schutz
- Maßnahmen/Pflichten

des Verantwortlichen und Maßnahmen zur Datensicherung

- Regelungen zum Umgang mit dienstlichen und privaten IT-Systemen zu dienstlichen Zwecken
- Anforderungen an die Auftragsverarbeitung, die Überprüfung der technischen und organisatorischen Maßnahmen sowie die Überprüfung des Auftragsverarbeiters durch den Verantwortlichen

Die Regelungen dieser Durchführungsverordnung sind unverzüglich, spätestens jedoch bis zum 31.12.2019, umzusetzen.

Orientierungshilfe zum Gesundheitsdatenschutz

Das Bundesministerium für Wirtschaft und Energie (BMWi) veröffentlichte eine „Orientierungshilfe zum Gesundheitsdatenschutz“ (Stand 2018-11). Die Orientierungshilfe richtet sich primär an Unternehmen, die Gesundheitsdaten für digitale Produkte verarbeiten. Dementsprechend ist der Text so verfasst worden, dass auch Nicht-Juristen gute Chancen haben, den Text zu verstehen. Inhalte der Orientierungshilfe sind

rechtliche Rahmenbedingungen, der Umgang mit Daten die unter § 203 StGB fallen, die Rolle der Auftragsverarbeiter, Gesundheits-Apps und vieles mehr. Die Orientierungshilfe kann auf der Internetseite des BvD heruntergeladen werden.



i Quelle: https://de.wikipedia.org/wiki/Gesetz_zum_Schutz_von_Gesch%C3%A4ftsgeheimnissen

i Quelle: <https://t3n.de/news/geschaeftsgeheimnisgesetz-1152086/>

i Quelle: <https://www.adorgasolutions.de/geschaeftsgeheimnisgesetz-geschgeh-verabschiedet/>

i Quelle: https://www.lida.bayern.de/media/FAQ_Zip.pdf

i Quelle: <https://www.kvhessen.de/kv-safenet/>

Bundestag beschließt Geschäftsgeheimnisgesetz

Das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) soll dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung dienen. Mit der EU-Richtlinie 2016/943 über den Schutz vertraulichen Know-Hows und vertraulicher Geschäftsinformationen ist bereits seit rund drei Jahren eine entsprechende Regelung in Kraft. Ende März hat der Deutsche Bundestag – mit mehrmonatiger Verzögerung – das GeschGehG beschlossen

und damit die EU-Richtlinie in deutsches Recht umgesetzt. Auch der Bundesrat hat nun zugestimmt und so kann das Gesetz am Tag seiner Verkündung im Bundesgesetzblatt in Kraft treten.

Bislang war der Schutz von Geschäfts- und Betriebsgeheimnissen in §§ 17 ff. UWG (Gesetz gegen den unlauteren Wettbewerb) geregelt. Die §§ 17 bis 19 UWG werden auf Grund des Sachzusammenhangs in das GeschGehG übernommen und mit dessen

in Kraft treten aufgehoben.

Das Gesetz zwingt Unternehmen, die ihre Geheimnisse schützen wollen, zu einem umfassenden Schutzkonzept. Unternehmen müssen Maßnahmen treffen, die zum Teil an die technischen und organisatorischen Maßnahmen erinnern, die sie aufgrund der DSGVO getroffen haben. Unternehmen, welche die DSGVO richtig umgesetzt haben, können daher auf bestehende Strukturen und Synergien zurückgreifen.

Verschlüsselung der E-Mail Kommunikation

Sensible personenbezogene Daten, insbesondere Gesundheitsdaten oder Sozialdaten, dürfen nicht unverschlüsselt per E-Mail übermittelt werden.

Der Beauftragte der Evangelischen Kirche Deutschland und auch das Bayerische Landesamt für Datenschutzaufsicht haben u.a. Stellung zur Übermittlung von Daten mittels verschlüsselter Zip-Datei genommen. Letztes hat in seinen FAQ zur DS-GVO Stellung zur Übermittlung von Patientenunterlagen als passwortschützte ZIP-Datei bezogen und die nachstehenden Voraussetzungen für eine Übermittlung per E-Mail genannt:

- Der E-Mailversand selbst muss transportverschlüsselt (TLS op-

portunistisch) erfolgen – technisch schwierig in der Umsetzung, da die Konfiguration beim Sender und beim Empfänger notwendig ist.

- Das Passwort, mit dem die ZIP-Datei geschützt ist, muss ausreichend komplex und mindestens 12-stellig sein.
- Bei der ZIP-Verschlüsselung muss die Einstellung AES-256 verwendet werden.
- Die Übermittlung des Passworts muss auf einem geeigneten Kommunikationskanal erfolgen (nicht auch per Email, z.B. persönlich, telefonisch, SMS, Messenger).
- Es darf dasselbe Passwort nicht an verschiedene Benutzer vergeben werden – jeder Benutzer muss ein eigenes Passwort erhalten.

Aus Sicht der Informationssicherheit ist dies allerdings bedenklich, denn im Unternehmen eingesetzte Scan-Verfahren können so kritische E-Mails und Anhänge aufgrund der Verschlüsselung nicht mehr herausfiltern. Es kann auch sein, dass solche E-Mails und verschlüsselten Anhänge gar nicht erst dem Empfänger zugestellt werden. Was also tun? Es gibt weitere Möglichkeiten, sensible Daten sicher zu übermitteln, um sowohl dem Datenschutz als auch der Informationssicherheit gerecht zu werden:

KV-Safenet: Hierbei handelt es sich um das sichere Netz der Kassenärztlichen Vereinigungen (SNK), mit dem Ärzte

und Psychotherapeuten eine gesicherte Verbindung über einen speziell konfigurierten KV-Safe-Net-Router aufbauen. So kommunizieren sie in einem vom Internet abgeschotteten Netz (VPN,

virtuelles privates Netz).

Cloud-Lösung: Einsatz einer gesicherten privaten Cloudlösung zum Datenaustausch z.B. Nextcloud.

Welche Lösung letztendlich geeignet ist muss unternehmensintern und individuell geprüft werden.

St. Franziskus-Stiftung Münster vernetzt sich mit TK-Safe

Die St. Franziskus-Stiftung Münster wird als erster Klinikverbund im Münsterland mit der elektronischen Gesundheitsakte der Techniker Krankenkasse (TK) TK-Safe vernetzt. Auf eine vertrauensvolle Zusammenarbeit haben sich die Vertragsparteien in einer gemeinsamen Absichtserklärung geeinigt. In Zukunft ist es den Teilnehmern möglich, Gesundheitsdaten in eine elektronische Gesund-

heitsakte (als App auf dem Mobiltelefon) übertragen zu lassen. Somit werden dem Patienten die eigenen medizinischen Informationen direkt zugänglich gemacht, was für mehr Transparenz sorgen soll. Es ist dann auch möglich, die Daten zur Einsicht freizugeben. Das entscheidet aber einzig und allein der Patient selbst. Denn weder die TK noch der Mitentwickler von TK-Safe, die IBM Deutschland GmbH,

können darauf zugreifen. Dafür sorgt eine individuelle Verschlüsselung, die direkt an der Quelle fungiert. Nur der Versicherte kann die Daten mit seinem persönlichen Schlüssel öffnen und einsehen. Damit ist TK-Safe ein digitaler Datentresor, dessen gesamte Datenehaltung in einem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierten Rechenzentrum bei der IBM in Deutschland erfolgt.



Quelle: <https://www.kma-online.de/aktuelles/klinik-news/detail/st-franziskus-stiftung-muenster-kooperiert-mit-tk-safe-a-39872>

Bewertung von Messengerdiensten aus Datenschutzsicht

Die Konferenz der Diözesandatenschutzbeauftragten der Katholischen Kirche Deutschland hat einen Kriterienkatalog zur Beurteilung von Messengern und anderen Social Media-Diensten verabschiedet. Jeder

Überprüfbarkeit durch Offenlegung der Algorithmen, Datenminimierung sowie der Wahrung der Rechte Dritter zu beurteilen.

Nach Ansicht der Konferenz der Diözesandatenschutzbeauftragten (DDSB)

lassen sich die datenschutzrelevanten Anforderungen an Messenger-Dienste auf die folgenden fünf Kriterien

verdichten:

• **Serverstandort:** Wo verarbeitet der Dienst-Anbieter die Nutzerdaten?

Hält der Provider die Drittlandbestimmungen ein, d. h. keine Datenspeicherung außerhalb der EU bzw. nur in Ländern, deren Datenschutzniveau durch die EU anerkannt ist?

• **Sicherer Datentransport:** Werden die Inhalte der Kommunikation Ende-zu-Ende verschlüsselt, also z.B. auch bei der Zwischenpufferung auf dem Server des Providers?

• **Überprüfbarkeit:** Verwendet der Anbieter ein Open-Source-Modell für die Implementierung seines Produktes, einschließlich des Einsatzes anerkannter und standardisierter Kryptogra-



Quelle: <https://www.katholisches-daten-schutzzentrum.de/bewertung-von-messengerdiensten-aus-daten-schutzsicht/>



Dienst ist demnach unter den Gesichtspunkten Serverstandort, Sicherheit des Datentransports,

Jeder Messenger- und Social-Media-Dienst ist hinsichtlich der Einhaltung des Datenschutzes zu beurteilen

i Quelle: <https://www.katholisches-daten-schutzzentrum.de/spende-als-letzter-wille-was-duerfen-angehoerige-erfahren/>

keine Weitergabe der Spendernamen ohne Einwilligung erlaubt

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

phie-Verfahren?

- **Datenminimierung:**

Werden die Metadaten der Verbindung so bald wie möglich gelöscht?

- **Respektierung der Rechte Dritter:** Werden nur die Kontaktdaten der an der Kommunikation Beteiligten verwendet und behält der Anwender die Kontrolle über sein Telefonbuch, oder wird z.B. das komplette Telefonbuch an den Provider übermittelt und

die Verantwortung für die Information der Betroffenen auf den Anwender abgewälzt?

Weitere Kriterien, die allerdings nicht mit Überlegungen zum Datenschutz begründet werden können, sind die Kosten und das jeweilige Lizenzmodell, welches evtl. einen Einsatz des Produktes im nicht-privaten Umfeld gar nicht zulässt.

Der Beauftragte für den Datenschutz der Evange-

lischen Kirche Deutschlands (EKD) hat am 30. Oktober 2018 eine frühere Stellungnahme aus Mai 2017 zum gleichen Thema ergänzt und trifft dabei vergleichbare Aussagen wie die Konferenz der DDSB. Auch andere Datenschutzaufsichten haben sich mit dem Thema mit immer wieder ähnlichen Ergebnissen beschäftigt.

Spende als letzter Wille – was Angehörige erfahren dürfen

Immer häufiger wird in Trauernachrichten und –anzeigen darum gebeten, dem Wunsch der verstorbenen Person entsprechend auf Blumen oder Kränze zu verzichten und stattdessen an eine caritative Einrichtung zu spenden. In den meisten Fällen veröffentlichen die Angehörigen nach vorheriger Absprache mit der Einrichtung die Kontoverbindung des Empfängers in der Traueranzeige. Wenn dann die Angehörigen einige Zeit später bei der bedachten Einrichtung um Offenlegung der Spenderliste mit Namen und den jeweiligen Beträgen bitten, stellt sich die Frage der Zulässigkeit dieser Informationsbereitstellung.

Für eine Übermittlung von personenbezogenen Daten (wozu Name und Spendenbetrag gehören) wird eine Rechtsgrundlage benötigt. Eine Erlaub-

nisgrundlage wäre gem. § 6 Abs. 1 lit. c KDG eine Vertragsbeziehung. Diese besteht durch die Durchführung der Überweisung aber nur zwischen dem Spender und dem Empfänger und hat i.d.R. nur den Zweck der Erstellung einer Spendenbescheinigung für das Finanzamt und die Verbuchung der Spende.

Die zweite Möglichkeit wäre das berechtigte Interesse der Angehörigen, wenn der Schutz der Interessen oder die Grundrechte des Spenders nicht entgegenstehen. Das Interesse der Angehörigen liegt möglicherweise darin, dass sie sich beim Spender persönlich bedanken möchten. Der Spender allerdings hat vielleicht ein Anliegen daran gegenüber den Angehörigen unbekannt zu bleiben. Nach Abwägung kommt man zu dem Ergebnis, dass das Interesse an der Anonymität des

Spenders überwiegt. Zuletzt könnte die Einwilligung nach § 6 Abs. 1 lit. b KDG in Betracht kommen. Diese muss jedoch aktiv erfolgen und mit allen erforderlichen Informationen versehen sein. Deshalb scheidet auch die Einwilligung als Rechtsgrundlage aus.

Fazit: Die Angehörigen müssen sich mit der Gesamtsumme der eingegangenen Spenden zufriedengeben und können sich natürlich in Form einer allgemeinen Dank-sagung bei den Spendern bedanken.

Impressum
FAC'T GmbH
Hohenzollernring 70
48145 Münster

info@factpartner.de
www.factpartner.de

Telefon 0251 935-3700
Telefax 0251 935-4075