Juli 2025 | Zum Datenschutz aufgefallen

Information zum (Weblink)
Datenschutz - Service
oder Fragen per Mail an:
Mail2@volkerschroer.de

Die Informationen wurden von mir sorgfältig zusammengestellt und beruhen auf öffentlich, zugänglichen Quellen, für die ich keine Gewähr auf Richtigkeit und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männlichen Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in)*,

Datenschutz → einfach praktisch hilfreich!

Wenn die Grundlagen einmal gelegt, sind die Abläufe meist schlank(er), der Aufwand gering und mit (der) Sicherheit mehr Zeit gewonnen. Datenschutz schafft Vertrauen und ist eine Grundlage für nachhaltigen Erfolg.

Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, Datenschutzmanagement bis zertifizierter, externer Datenschutzbeauftragter für Selbstständige, Gewerbetreibende und KMU.

Sprechen wir!

Vielen Dank für Ihr Interesse

PS: Nutzen Sie die Möglichkeit nur zu lesen, was für Sie von Interesse ist, oder kontaktieren Sie mich gerne.

Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.1a.....1
2. Zum Datenschutz.....1
a) Datenverarbeitung des Betriebsarztes.....1
b) Hinweis zum Datentransfer mit den USA.....2
3. Zur Datensicherheit.....3
a) E-Mails, ohne geht es nicht, aber …!.....3
(1) Bedrohungsszenarien.....3
(2) Schutzmaßnahmen.....3
(3) Empfehlungen für Organisationen.....3
4. Zu angrenzenden Themen.....3
a) Mal einen Blick auf Geldbußen für DSGVO-Verstöße in Deutschland 2025.....3
(1) € 45 Mio. „unzureichend“.....3
(2) € 120.000 „verspätet“.....3
(3) € 30.000 „unerlaubt“.....3

1. Standard – Datenschutz – Modell Vers. 3.1a

Standard-Datenschutz-Modell
übersichtlich zusammengefasst
11 Seiten

Standard-Datenschutz-Modell
Datenschutzkonferenz DSK
78 Seiten

Datenschutz-Grundverordnung
auf dejure.org

Bundesdaten-schutzgesetz
auf dejure.org

Das SDM [*der Datenschutzkonferenz der Aufsichtsbehörden des Bundes und der Länder (DSK)*] überführt die rechtlichen Anforderungen der DS-GVO über 7 Gewährleistungsziele in die technischen / organisatorischen Maßnahmen zur Unterstützung der Transformation abstrakter – rechtlicher Anforderungen in konkrete Maßnahmen. Ziel ist, eine gemeinsame Sprache der Juristen und Informatiker für die Verantwortlichen und Datenschutzpraktiker zu finden.
| Aktuell: SDM Version 3.1a (05/2025) Änderung Logo, einzelne grafische Darstellungen, keine inhaltlichen Änderungen
| Letzter Maßnahmenkatalog 11/2021: Nr.51 „Zugriff auf Daten, Systeme und Prozesse regeln.“

2. Zum Datenschutz

a) Datenverarbeitung des Betriebsarztes

Im „Netzwerk Datenschutzexpertise“[1] gibt es eine Interessante rechtliche Betrachtung zur Datenverarbeitung von Betriebsärzten.[2] Die Komplexität kann ich nicht besser zusammenfassen:

Die betriebsärztliche Datenverarbeitung und die damit verbundene Dokumentation von Gesundheitsdaten weist gegenüber sonstigen Formen ärztlicher Datenverarbeitung eine Besonderheit auf: Nicht nur das Medizinrecht und das Datenschutzrecht kommen zur Anwendung, sondern zudem das Arbeitsrecht, das Mitbestimmungsrecht und die dort bestehenden spezifischen Regelungen. Mit der Wirksamkeit der Europäischen Datenschutz-Grundverordnung kam ergänzend zu den nationalen Regelungen eine europäische Regelungsebene hinzu. *(Zitat siehe LINK Einleitung zu „Die Datenverarbeitung des Betriebsarztes“)*

1 *Link: https://www.netzwerk-datenschutzexpertise.de/*
2 *Quelle: Netzwerk Datenschutzexpertise: „Die Datenverarbeitung des Betriebsarztes“*

Von mir hier nur ein paar grundlegende Dinge. Mit dem Behandlungsvertrag gilt das Arzt-Patienten-verhältnis und die ärztliche Schweigepflicht. Die Betriebsärzte sind gegenüber den Arbeitgebern weisungsfrei, d. h. eine Weitergabe von Gesundheitsdaten bedingt immer eine gesetzliche Verpflichtung (z. B. Arbeitssicherheit) oder eine gesetzliche Befugnis (z. B. Einwilligung).

Für die Verarbeitung besonderer Kategorien (u. a. Gesundheitsdaten) personenbezogener Daten gelten die Vorschriften Art.24, 25 DSGVO und § 22 BDSG, die zur Datensicherheit vorgeschriebenen technischen und organisatorischen Maßnahmen unter Berücksichtigung des Stands der Technik und der Implementierungskosten im Verhältnis zum Risiko für die Betroffenen. Jetzt gibt es dazu keine konkreteren Ausführungen, aber festgehalten werden kann:

- Verantwortlich sind bei externen Betriebsärzte:innen sie selbst und bei internen der Arbeitgeber. Für die Daten gilt immer die ärztliche Schweigepflicht.
- Nicht zu vergessen, dass auch für die papierhafte Dokumentation entsprechende technische und organisatorische Maßnahmen zum Schutz vor dem Zugriff / Zugang von Dritten zu treffen sind.
- Entscheiden für mich ist, dass bei der elektronischen Verarbeitung eine Verschlüsselung der Daten vorgenommen wird (mindestens eine Zugriffsbegrenzung / -berechtigung nur für Betriebsärzte:innen und Hilfspersonal).
- Die IT-Dienstleister der Betriebsärzte:innen sind „Gehilfen“ oder „Mitwirkende“ im Sinne des § 203 Abs.1 StGB (Verletzung von Privatgeheimnissen) und unterliegen der ärztlichen Schweigepflicht. Stellt der Arbeitgeber die IT-Dienstleistung, sind die Administratoren auf die Schweigepflicht hinzuweisen!
- Auch bei IT-Administratoren sollte der Zugriff auf eine Mindestmaß beschränkt werden.

b) *Hinweis zum Datentransfer mit den USA*

Es ist schon schön bequem, wenn ein angemessenes Schutzniveau nach DSGVO in dem Land der Datenverarbeitung der Organisation vorherrscht, dass durch die EU geprüft und mit einem Angemessenheitsbeschluss bestätigt ist (Art.45 DSGVO Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses). Dieser Angemessenheitsbeschluss der EU für die USA, der einen vereinfachten Datenaustausch zwischen der EU und den USA ermöglicht, steht unter Beobachtung und könnte durch rechtliche Herausforderungen und politische Entwicklungen gefährdet sein. Ausführungen dazu am Beispiel der Artikel:

- **„*Trump bedroht wichtigen Daten-Deal – Wirtschaft schlägt Alarm*“ (Handelsblatt 03/25)**[3]. Unter anderem wurden alle Mitarbeiter eines für den Datenschutz zentralen Gremiums, dem „Privacy and Civil Liberties Oversight Board (PCLOB)“, bis auf einen Mitarbeiter entlassen.
- **„*Trump könnte Microsoft und Meta zwingen, Europa zu verlassen*“ (INFOsperber 05/25)**[4]. Wie alle anderen Anbieter aus den USA auch.
- **„*Microsoft kann US-Zugriff auf EU-Cloud nicht verhindern*“ (Dr. Datenschutz 07/25)**[5]. So der Chefjustiziar von Microsoft France bei einer öffentlichen Anhörung vor dem französischen Senat des Parlaments zu.

Es gibt derzeit mehrere Klagen und Beschwerden gegen die Datenübermittlung zwischen der EU und den USA, insbesondere im Zusammenhang mit dem „EU-US Data Privacy Framework (DPF)“. Diese beziehen sich hauptsächlich auf die Frage, ob das Datenschutzniveau in den USA ausreichend ist, um den Anforderungen der Europäischen Datenschutzgrundverordnung (DSGVO) zu genügen. Nur auf das Prinzip: „Hoffnung“ zu setzten, kann und ist mit recht großen Risiken verbunden. Mit Plan B sollten mögliche Risiken gelindert (bis vermieden) werden. Ansätze:

- Basiert der aktuelle Datentransfer in die USA auf der Grundlage des „EU-US Data Privacy Frameworks“ sollte die Vereinbarung möglichst um die EU-Standardvertragsklauseln erweitert werden. Diese treten nur in Kraft, wenn der Angemessenheitsbeschluss der EU für

3 *Quelle: Handelsblatt: „Trump bedroht wichtigen Daten-Deal – Wirtschaft schlägt Alarm.“*
4 *Quelle. INFOsperber: „Trump könnte Microsoft und Meta zwingen, Europa zu verlassen“*
5 *Quelle: Intersoft consulting: „Microsoft kann US-Zugriff auf EU-Cloud nicht verhindern!“*

die USA entfällt (temporäres Sicherheitsnetz).

► Es ist hilfreich, sich bereits jetzt nach alternativen Anbieter aus Europa umzuschauen. Das ist keine leichte Aufgabe und wird Zeit brauchen, den richtigen Anbieter für sich zu finden. Einige namhafte Akteure sind bereits auf dem Weg, wie der Presse zu entnehmen. Zwei Beispiele:

→ Schleswig-Holstein macht LibreOffice zur Standard-Office-Lösung in der Verwaltung und setzt auf das Betriebssystem Linux[6].

→ LibreOffice ersetzt Microsoft 365 in der dänischen Regierung: eine strategische Wende[7].

Man muss nicht „mit der Brechstange“ an das Thema gehen, aber ein „Plan B“ kann nicht schaden.

3. Zur Datensicherheit

a) *E-Mails, ohne geht es nicht, aber …!*

Es ist kein Geheimnis, E-Mails gehören zum beruflichen und privaten Alltag und sind da auch nicht wegzudenken. Genau deswegen, sind E-Mails ein beliebtes Ziel für Betrüger und Hacker. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat neue Empfehlungen veröffentlicht[8]. Ein Blick der sich lohnt, um sich vor Datenklau, Betrug und Imageschäden zu schützen. Die Seite des BSI bietet einen umfassenden Überblick über Risiken im E-Mail-Verkehr und entsprechende Schutzmaßnahmen für Organisationen. Hier sind die wichtigsten Punkte:

(1) Bedrohungsszenarien

- **Schadsoftware-Infektionen:** E-Mails mit gefährlichen Anhängen oder Links sind häufige Einfallstore für Malware.
- **Datenabfluss & Manipulation:** Unverschlüsselte E-Mails können abgefangen, mitgelesen oder verändert werden.

(2) Schutzmaßnahmen

- **Verschlüsselung:** Zum Schutz von Vertraulichkeit und Integrität.
- **Digitale Signaturen:** Zur Sicherstellung der Authentizität von Absendern.
- **Spam-Abwehr:** Reduziert unerwünschte E-Mails und entlastet die Infrastruktur.

(3) Empfehlungen für Organisationen

- **IT-Grundschutz-Kompendium:** Enthält Bausteine und Standards zur Absicherung von E-Mail-Clients und -Servern (z. B. Microsoft Outlook, Exchange).
- **ISi-Reihe (Internet-Sicherheit):** Bietet technische und nicht-technische Leitfäden zur sicheren Nutzung und zum sicheren Betrieb von E-Mail-Systemen.

Unter den technischen Leitfäden befindet sich auch eine nicht-technische Kurzfassung für (IT-) Manager (Links): Sichere Nutzung von E-Mail (Isi-L), sicherer Betrieb von E-Mail-Servern (Isi-L).

4. Zu angrenzenden Themen

a) *Mal einen Blick auf Geldbußen für DSGVO-Verstöße in Deutschland 2025*

(1) € 45 Mio. „unzureichend“
Unzureichende Überprüfung und Überwachung von Unterauftragnehmern (Details)

(2) € 120.000 „verspätet“
Drastisch verspätete Reaktion auf Auskunftsersuchen (Details)

(3) € 30.000 „unerlaubt“
Unerlaubte Videoüberwachung (Details)

Bei Bedarf, einfach mal sprechen!

6 Quelle: OSB ALLIANCE: „Schleswig-Holstein macht LibreOffice zur Standard Office-Lösung in der Verwaltung“
7 Quelle: hfrance.fr/de: „LibreOffice ersetzt Microsoft 365 in der dänischen Regierung: eine strategische Wende“
8 Quelle: BSI: „E-Mail-Sicherheit“