Datenschutz im Gesundheitswesen

Besondere Daten bedürfen besonderen Schutz!

Gesundheitsdaten zählen aus Sicht des Datenschutzes zu den besonderen Arten personenbezogener Daten und werden nicht nur in der Datenschutzgrundverordnung (DSGVO) als sehr schützenswert eingestuft – vor allem weil der Verlust oder gar der Missbrauch solch sensibler Informationen, erhebliche Konsequenzen nach sich zieht. Beispielsweise könnte durch eine Veröffentlichung der Daten, Einfluss auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse eines Betroffenen genommen werden.

In den letzten Jahren gewinnt die Cyberkriminalität zudem an Bedeutung. Hier werden, beispielsweise durch den Einsatz von Ransomware, u. a. Krankenkassen, Kliniken, Pflegeeinrichtungen und Arztpraxen immer wieder in den Fokus genommen, um an sensible Gesundheitsdaten heranzukommen.

Aber nicht nur für Einrichtungen und Personen, die direkt im Gesundheitswesen tätig sind, ist im Umgang mit Gesundheitsdaten enorme Vorsicht geboten, sondern auch bei jedem verantwortungsbewussten Unternehmen. Auch hier gilt es, alle Möglichkeiten zu nutzen, um ein höchstmögliches Sicherheitsniveau zu garantieren. Zudem sollten regelmäßige Schulungen dafür Sorge tragen, dass das Personal optimal auf alle Gegebenheiten vorbereitet ist, z. B. im Umgang mit riskanten E-Mails. Diese sollten eigenständig erkannt und eliminiert werden.

Um auch Ihnen einen ersten Überblick zu geben, was Gesundheitsdaten sind, wie man diese am besten schützt und welche Maßnahmen hilfreich sind, bieten wir Ihnen sehr gerne einen für Sie

kostenfreien Beratungstermin.

In diesem klären wir gemeinsam alle Risiken, gehen auf die gesetzlichen Vorgaben ein und geben Ihnen Handlungsempfehlungen, mit denen auch Sie weiterhin rechtssicher agieren können.

Antwort

Ja, wir hätten gerne eine Beratung zum Thema Datenschutz im Allgemeinen oder im Speziellen zum Thema Datenschutz im Gesundheitswesen.

	Ja	Nein
Wir hätten gerne eine Beratung zum Thema Datenschutz im Gesundheitswesen.	☐	☐
Wir haben Maßnahmen umgesetzt, möchten diese aber gerne von einer unabhängigen Stelle prüfen lassen.	☐	☐
Wir haben bereits einen betrieblichen oder externen Datenschutzbeauftragten.	☐	☐

Firma

Straße

PLZ | Ort

Telefon

Ansprechpartner

E-Mail

Bitte senden Sie diese unverbindliche Anfrage an:

Datenschutz für Unternehmen

Datenschutz im Gesundheitswesen

Was versteht man unter Gesundheitsdaten?

Um festzulegen wie Gesundheitsdaten definiert sind, schauen wir uns den Art. 4 Nr. 15 der DSGVO an. Hier steht zur Begriffsbestimmung folgendes:

„… personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen …“

Hinzu können genetische Daten kommen (Art. 4 Nr. 13 DSGVO). Auch muss der Art. 9 DSGVO (Verarbeitung besonderer Kategorien pers. Daten) Abs. 1 in alle Überlegungen mit einbezogen werden:

„… Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt. …“

Durch diese Vorgaben wird bestimmt, was Gesundheitsdaten im Allgemeinen sind. Zudem werden sie als besonders schützenswert eingestuft, wodurch sie ohne ausdrückliche Einwilligung der Betroffenen nicht so einfach verarbeitet und gespeichert werden dürfen. Hierbei gibt es natürlich Ausnahmen. Beispielsweise, dann wenn die Verarbeitung „zum Schutz lebenswichtiger Interessen“ oder zum „Recht der sozialen Sicherheit“ durchgeführt werden muss.

Die Hürden sind allerdings hoch und somit muss bei einer möglichen Verarbeitung von Gesundheitsdaten immer eine Einwilligung der betroffenen Person oder eine Rechtsgrundlage vorliegen!

Ärztliche Schweigepflicht vs. Datenschutz!

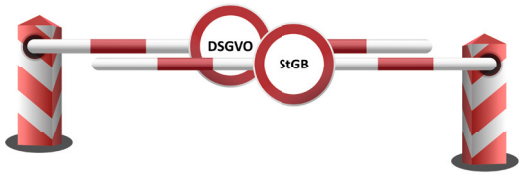
Die ärztliche Schweigepflicht wird durch den § 203 StGB festgeschrieben. Hier wird im Abs. 1 StGB bestimmt, dass

„… derjenige, der unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als Arzt anvertraut oder sonst bekannt geworden ist, mit Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe bestraft wird. …“

Dies gilt zudem für berufsmäßig tätige Gehilfen und die zur Vorbereitung auf den Beruf tätigen Personen, was neben den Ärzten auch Apotheker, Krankenschwestern, Arzthelfer etc. miteinschließt. Ferner werden hier alle berufsnahen Gehilfen (Sekretariat, Sprechstundenhilfen uvm.) explizit angesprochen.

Reicht das aus Sicht des Datenschutzes?

Das Vorhandensein einer beruflichen Ethik, selbst wenn diese gesetzlich oder in einer Berufsordnung geregelt ist, **entbindet nicht von der Pflicht, alle Datenschutzvorschriften zu beachten** – „Zwei-Schranken-Prinzip“!



Somit ist die Schweigepflicht alleine keine ausreichende Grundlage, um Gesundheitsdaten zu erheben, zu verarbeiten oder zu speichern. Zulässig ist die Verarbeitung nur dann, wenn auch die DSGVO oder eine andere Rechtsvorschrift dies erlaubt oder vorschreibt, oder Betroffene selbst ihre Einwilligung erteilt haben.

Die zum Schutz von sensiblen Daten nötigen tech. und organisatorischen Maßnahmen (TOM) sind immer dort ohne Einschränkung umzusetzen, wo Gesundheitsdaten verarbeitet werden!

Fotos: www.pixabay.com

TOM im Gesundheitswesen

Sicherheit der Verarbeitung

Die Basis für technische und organisatorische Maßnahmen (TOM), die getroffen werden müssen, bildet der Art. 32 der Datenschutzgrundverordnung:

„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 Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“

Hieraus kann ein erster Maßnahmenplan erarbeitet werden, der u. a. folgende Themen abdecken sollte:

- Datenschutz am Empfang (Diskretionszone)
- Datenschutz im Wartebereich
- Datenschutz im Behandlungsbereich
- Datenschutz in der Verwaltung
- Tech. Maßnahmen - Informationstechnologie
- Grundlegende Maßnahmen - Personal
- Maßnahmen bei Datenübermittlungen

Fazit | Wir helfen sehr gerne!

Falls Sie mehr über Datenschutz im Gesundheitswesen wissen möchten, können Sie gerne unsere aktuelle Datenschutzzeitung anfordern. Mit dieser erhalten Sie weitere Informationen zum Thema, können mit einer ersten Selbsteinschätzung Ihre tech. und organisatorischen Maßnahmen prüfen und erfahren warum eine Praxis 105.000 EUR Bußgeld bezahlen musste. Zudem bieten wir Ihnen sehr gerne einen Beratungstermin an, in dem wir gemeinsam alle Risiken klären und Handlungsempfehlungen benennen mit denen auch Sie weiterhin rechtssicher agieren können.