Januar 2022 | 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 Richtig- und Vollständigkeit übernehmen kann.
*) Aus Gründen der besseren Lesbarkeit Verwendung der männliche Form, die alle Geschlechter mit einbezieht.

Liebe(r) Leser(in),*

Datenschutz → praktisch einfach und hilfreich!

Wenn die Grundlagen gelegt, sind die Abläufe meist verschlankt, der Aufwand verringert und mit (der) Sicherheit mehr Zeit gewonnen. Einfach praktisch!

Datenschutz schafft Vertrauen und ist eine der Grundlagen für nachhaltigen Erfolg.

Wie einleitend im Standard – Datenschutz – Modell der Datenschutzkonferenz festgehalten, „müssen Juristen und Informatiker deshalb eine gemeinsame Sprache finden“ . Mein Ziel ist es, den Datenschutz einfach, praktisch und hilfreich zu vermitteln und zu gestalten. Von Datenschutzberater, Datenschutzberatung, Datenschutzmanagement bis zertifizierter, externer Datenschutzbeauftragter für Selbständige, 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. 2.0b

Mit dem SDM verfolgt die Datenschutzkonferenz (DSK) der Aufsichtsbehörden des Bundes und der Länder eine „gemeinsame Sprache der Juristen und Informatiker“ für die Verantwortlichen und Datenschutzpraktiker zu finden. Letzte Fassung vom 17.04.2020

Zum aktuellen SDM der Aufsicht (72 Seiten; Link in Bild & Text)	**Zur Zusammenfassung des SDM (10 Seiten; Link in Bild & Text)**

Letzte Ergänzung: 11/2021: Baustein 51 (zu TOM)

Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“ (Version 1.0 vom 01.11.2021)[1].

2. Zum Datenschutz

(a) Patienten – Daten – Schutz – Gesetz (PDSG)

Das Ärzte, Labore und Kliniken bereits einen hohen (mehrheitlich internen) Digitalisierungsgrad aufweisen, haben leider die Cyberangriffe der letzten Jahre gezeigt. Auf der anderen Seite besteht ein erheblicher Mangel in der digitalen Kommunikation mit Dritten, z. B. mit den Patienten. Daraus folgt die Forderung nach: ***„Transformation, aber mit Sicherheit!“***, zumal Datenschutz-Grundverordnung (DS-GVO) und Bundesdatenschutzgesetz (BDSG) medizinische Daten unter besonderen Schutz gestellt wissen wollen. Festgehalten im fünften Buch der Sozialgesetzgebung Kapitel 10 und 11 (Abk. SGB V §284ff und §306ff)[2]. Einen kurzen Überblick der wesentlichen Inhalte gibt es hier – wie immer mit Angaben zu Quellen und Link - als PDF aus 3 Seiten:

1 *Quelle: SDM – Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln" Zusammenfassung (PDF 1 Seite) Zur Vollversion der Veröffentlichung der Datenschutzkonferenz (PDF 23 Seiten)*

2 *Quelle: https://dejure.org/gesetze/SGB_V/284.html <> https://dejure.org/gesetze/SGB_V/306.html*

https://volkerschroer.de/DSGVO/2022.01.10.PDSG-kurzgefasst.pdf.

i) PDSG und Datenschutz

Bereits vor der Pandemie war der Ruf nach digitaler Transformation im Gesundheitswesen groß und die Diskussion um die Sicherheit der Daten aus allen Richtungen groß und führte zu Änderungen des ersten Entwurfs. Im Bundesgesetzblatt 2021 Teil 1 Nr. 28 vom 08.06.21 ist sogar eine Datenschutz – Folgenabschätzung als Anlage zu §307 mitveröffentlicht[3]. Mit Schreiben vom 16/8/21 hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI Prof. U. Kleber) einen Musterbescheid an die gesetzlichen Krankenkasse verschickt und eine Pressemitteilung am 19/8/21 veröffentlicht[4].

ii) Gesetzeskonflikte oder Umsetzungsmangel?

(Umsetzungsmangel!) Wenn ich die Veröffentlichungen des BfDI richtig deute, dann liegt es an:

1. Das (sich verzögernde) fehlen eines „feingranularen Berechtigungsmanagement“, mit der Versicherte / Patienten den Zugriff bzw. die Freigaben bis auf jeden einzelnen Datensatz selbst regeln können, da die gemantik GmbH (zuständige für die sichere Telematikinfrastruktur) noch kein System freigegeben hat. Was ja noch kommen kann!
2. Die „sichere digitale Identität“ ist spätestens ab dem 01.01.2023 (SGB V §291) verfügbar zu machen, d. h. es ist noch etwas Zeit, bis ein geeignetes System gefunden wird.

Korrekt ist, dass derzeit ohne Frontend (Kartenlesegerät, Smartphone) ein Zugriff nicht möglich ist. Da finde ich den Vorschlag eines Zugriffs über ein Kartenlesegerät in den Filialen der Krankenkassen eine geniale Alternative.
Die Aufbewahrungsfristen für die Leistungserbringer (Krankassen, Ärzte usw.) für die notwendigen Abrechnungsdaten sind ja geregelt und alle anderen Dokumente werden ja vom Versicherten / Patienten selbst verwaltet. Eine elektronische Patientenakte basiert auf Freiwilligkeit und muss bei der Krankenversicherungen beantragt werden.

Also weniger ein Gesetzeskonflikt zwischen PDSG und BDSG / DS-GVO, als ein noch zeitlich, lösbarer Umsetzungsmangel (hoffentlich?!).

iii) IT – Sicherheit zum Patienten - Datenschutz

Im Gesetz als Telematik – Infrastruktur bezeichnet. Die von der gematik GmbH (Umsetzungsgesellschaft des Bundes und der Leistungserbringer) konzipierten Anwendungen werden mit dem Bundesbeauftragen für den Datenschutz und die Informationsfreiheit (BfDI) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt, auf der Grundlage des SGB V Kapitel 11. Damit das in den Konzepten geplante Sicherheitsniveau auch in der Umsetzung gewährleistet werden kann, zertifiziert das BSI wichtige Komponenten, nachdem die einzelnen Komponenten von anerkannten Prüfstellen nach den Schutzprofilen und technischen Richtlinien des BSI[5] evaluiert wurden[6].

(b) Angst vor dem Kunden?

Datenschützer und Verbraucherverbände gehen gegen die Datenweitergabe von Mobilfunkanbietern vor, berichtet die Tagesschau[7]. Ohne Aufklärung der Verbrauchers / Nutzers, geschweige denn einer Rechtsgrundlage, geben Mobilfunkanbieter (ohne die Telekom) Kundendaten (nicht Telefonate, sondern beispielsweise zum Vertragsabschluss, Vertragsdauer oder Vertragswechsel) an die Schufa weiter, zur Bewertung des Zahlungsverhaltens. „Warum werden wir nicht aufgeklärt? Da stimmt doch was nicht? Wo ist das Problem?“ Heimlichkeiten sind keine gute Strategie!

3 Quelle: Bundesgesetzblatt Nr. 28, 8.6.2021: Datenschutz – Folgenabschätzung (DSFA) zum PDSG, PDF ab Seite 42
4 Quelle: BfDI: Pressemitteilung zu Folgen der Gesetzgebung PDSG
5 Quelle: BSI: Schutzprofile und technische Richtlinien
6 Quelle: BSI: Telematikinfrastruktur – sichere Vernetzung medizinischer Versorgung
7 Quelle: Tagesschau: „Mobilfunkbetreiber gegen Datenschützer (und Verbraucherverbände)“

3. Zur Datensicherheit

(a) IT-Sicherheit im Gesundheitswesen(?)

In der „Sektorstudie Gesundheit“ des BSI[8] vom 22.11.2021, gibt es unter Punkte 6 auf den Seiten 170ff, eine Liste von Empfehlung zur Verbesserung der Sicherheit der IT im Gesundheitswesen an Betreiber, Innenministerium, Gesundheitsministerium, Bundesregierung und Verbände. Als akuten, technischen Handlungsbedarf (Probleme) sieht das BSI die Absicherung von

unkontrollierten Fernwartungszugängen, potentielle Schwachstellen in IT-basierten, insbesondere vernetzten Medizinprodukten, der Netzwerkzugangskontrollen / Mobil Device Management, medizinische wie nicht – medizinische Netzwerke und die Verschärfung der Anforderungen an Zutritts- und Zugriffskontrollen.

4. Zu angrenzenden Themen

(a) Aufsicht (AT): Google Analytics # DS-GVO [9]

Die österreichische Datenschutzbehörde hat einen (noch nicht rechtskräftigen) Bescheid zur Nutzung von Google Analytics durch Website – Betreiber erlassen. Durch die Nutzung des Tools auf der eigenen (verantwortlichen) Website entsteht ein einzigartiger, digitaler Fingerabdruck. Mangels Angemessenheitsbeschluss der EU und Maßnahmen für ein gleichwertiges Schutzniveau (schwer) ist ein Drittlandtransfer nicht erlaubt (Zitat: *„jedenfalls auf Grundlage des im Bescheid festgestellten Sachverhalts“*).

(b) Datenlecks in Schlagzeilen

Wie Tagesschau / Plusminus berichten[10], waren sensible Nutzerdaten von großen Plattformen OTTO, Kaufland, MediaMarkt, check24; Tyre24, idealo, Hood und Crowdfox jahrelang ungeschützt im Netz. Der Fehler wurde zwar 2021 behoben, die Daten (Mail- und Postadressen, Bestellinformationen, Telefonnummern, teilweise sogar Bankverbindungen) sind aber bereits im Darknet aufgetaucht. Betroffen sind ca. 700.000 Kunden. Die Plattformbetreiber verweisen zur datenschutzrechtlichen Haftung auf die Händler, sie seien ja nur Vermittler zu den Kunden ☹

(c) Datenpannen abseits der Schlagzeilen[11]

Es sind wohl nicht nur die „Großen“, denen Datenschutzverletzungen unterlaufen. Der LfDI – Schleswig – Holstein zieht das Fazit: „Wieder mehr Beschwerden, wieder mehr Datenpannen und vor allem mehr Angriffe auf den Datenschutz“. Die genannten Dauerbrenner:

- ✗ Home-Office: Weiterleiten von E-Mails an das private Mail – Konto
- ✗ Videoüberwachung: Fehlender u/o korrekter Hinweis, Löschroutine
- ✗ Corona Kontaktdaten: Von Dritten einsehbar, zusätzliche Informationen, Zweckentfremdung
- ✗ Unzureichende IT-Sicherheit: keine Verschlüsselung, Rücksicherungsmöglichkeit, Diebstahl
- ✗ Fehlversand/Verlust: Falscher Adressat und falscher Umgang bei Entdeckung
- ✗ Offene E-Mail-Verteiler und Umgang bei Entdeckung

(d) Feature?: Krypto-Miner von Avira & Norten

Doch bemerkenswert fand ich den Hinweis von WinFuture[12] unter Bezug auf mehrere andere Quellen, dass Norton und Avira über ihre Sicherheitssoftware auch Crypto - Miner installieren, die sich im Leerlauf ihres Rechners den Kapazitäten bedienen. Die Ankündigung (evtl. Zustimmung?) haben viele Nutzer anscheinend nicht bemerkt. Über die Höhe der Einnahmen, geschweige den eines Nutzeranteils ist bisher nicht bekannt.

Bei Bedarf, einfach einmal sprechen!

8 Quelle: BSI: „Sektorstudie Gesundheit“
9 Quelle: dsb Rep. Österreich: TEILBESCHEID SPRUCH Datenschutzbeschwerde (PDF)
Dr. Datenschutz: „Google Analytics und das Datenübermittlungsproblem“
10 Quelle: Tagesschau / Plusminus: „Nutzerdaten jahrelang online“
11 Quelle: Security-Insider: „Datenpannen jenseits der Schlagzeilen“
12 Quelle: WinFuture: „Feature, nicht Trojaner: Avira und Norton installieren Krypto-Miner“