März 2026 | 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

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. Datenschutz und Datensicherheit

a) „Nichtverkettung“ im Datenschutz

(1) Ziel:

Die Vermeidung einer Zusammenführung (Verkettung) von Daten, die zu unterschiedlichen bzw. zu anderen Zwecken erhoben wurden (fehlender Rechtsgrund). Eine rechtliche, zulässige

Verkettung ist nur unter eng definierten Umständen möglich. Dies ist durch technische und organisatorische Maßnahmen (z. B. Pseudonymisierung, Anonymisierung, Berechtigungskonzepte) sicherzustellen.

(2) Rechtliche Anforderung

Die rechtliche Anforderung ergibt sich aus Art.5 Abs.1b der DS-GVO über die Grundsätze für die Verarbeitung personenbezogener Daten:

> *(1) Personenbezogene Daten müssen:*
> *(1) b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;*

und zu den eng definierten Umständen:

> *(1) b) eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken ("Zweckbindung");*

In Art.89 Abs.1 DS-GVO geht es um Garantie für die Verarbeitung der in Art.5 Abs. 1b genannten Ausnahmen. Auszug:

> *Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.*

(3) Praktische Anforderungen

Anwendungen, Systeme und Berechtigungen sollten so gestaltet sein, dass nur auf personenbezogene Daten zugegriffen werden kann, für die eine Rechtsgrundlage besteht.

(3.1) *Zweckbindung*

Daten, die für einen bestimmten Zweck erhoben werden, dürfen nicht einfach mit Daten für einen anderen Zweck kombiniert oder für einen ganz anderen Zweck genutzt werden.

(3.2) *Datentrennung*

Technisch und organisatorisch muss sichergestellt werden, dass Datenbestände aus unterschiedlichen Verarbeitungsprozessen getrennt bleiben.

(3.3) *Profiling*

Durch die Nichtverkettung ist zu verhindern, dass verschiedene Informationen aus unterschiedlichen Lebensbereichen zusammengeführt werden, was die Privatsphäre der betroffenen Personen stark beeinträchtigen könnte (Profiling ist mit weiteren Anforderungen verknüpft).

(3.4) *Beispiele für mögliche Verstöße*

- Erhalt von Kontaktdaten (Visitenkarte) sind keine, gleichzeitige Einwilligung in Werbung
- Und auch keine Einwilligung in der Verarbeitung / Speicherung bei oder durch Auftragsverarbeiter
- Personendaten aus erledigten und abgerechneten Verträgen sind zwar für die Finanzverwaltung nach GoBD entsprechend aufzubewahren (Rechtsgrund: Gesetz), dürfen aber nicht mehr für Werbung, Kontakt, Information u. ä verwendet werden, da dafür der Zweck entfallen ist.

(3.5) *Zusammenfassung:*

Zusammengefasst zielt die Nichtverkettung darauf ab, die Zweckbestimmung der Datenverarbeitung zu garantieren und die Erstellung von Persönlichkeitsprofilen durch die Zusammenführung isolierter Datenquellen zu verhindern.

3. Am Rande notiert

a) *Meta – Instagram beendet verschlüsselte Direktnachrichten*[1]

Meta schafft bei seinem Fotodienst Instagram die verschlüsselten Direktnachrichten ab. Die Begründung sei ein geringes Interesse der Nutzer. Eigentlich wollte Meta den Schutz privater Kommunikation nach Facebook und WhatsApp weiter ausbauen. Die bei Instagram erst vor wenigen Jahre eingeführte Funktion wird jetzt wieder abgeschafft. Laut Meta haben nur "sehr wenige" Menschen die verschlüsselten Chats genutzt, heißt es. Bevor die Funktion entfernt werde, sollten Anwender ihre bisherigen Chats und in Nachrichten geteilte Bilder sichern. Wer weiterhin verschlüsselt kommunizieren wolle, solle auf WhatsApp (*Anm.:„Super Tipp* 😒 “) ausweichen, heißt es. Laut "The Verge" fordern Behörden weltweit strengere Regeln für Online-Plattformen. Kritiker argumentierten, dass verschlüsselte Nachrichten es erschwerten, strafrechtliche Inhalte zu erkennen und zu melden. Ein Generalstaatsanwalt in den USA habe einen Antrag eingereicht, Meta zu verbieten, verschlüsselte Chats für Minderjährige anzubieten. Auch in Großbritannien gebe es Diskussionen über mögliche Zugriffe auf verschlüsselte Daten, heißt es.

b) *Trackt Microsoft illegal Minderjährige?*[2]

Die österreichische Datenschutzaufsicht hat scheinbar auf einem Schülerrechner mit Microsoft 365 Education rechtswidrige Tracking-Cookies ausgemacht. Diese sollen rechtswidrig installiert und persönliche Daten abgegriffen haben, obwohl zuvor in den Datenschutzeinstellungen wo immer möglich die Datenübermittlung abgelehnt wurde. Das könnte auch für alle anderen „365er“ kritisch werden. Der Bekannte „Schrems“ mit seiner Organisation noyb ist bereits mit Beschwerden bei der Schule, Schulbehörde und Datenschutzaufsicht involviert. Wir werden davon noch lesen und hören, bestimmt!

c) *Microsoft Word fliegt raus!*[3]

Deutschland macht das OpenDocument Format (ODF) zur Pflicht für die öffentliche Verwaltung im Rahmen des „Deutschland-Stacks“, um die digitale Souveränität zu stärken und die Abhängigkeit von proprietären Formaten (wie .docx) zu beenden. Bis 2028 müssen Dokumente im Austausch in ODF oder barrierefreien PDF/UA-Formaten erfolgen (IT-Planungsrat im Standard Rahmenwerk „Deutschland-Stack“). Bis 2028 ist die gesamte öffentliche Verwaltung (Bund, Länder, Kommunen) umzustellen bzw. haben Dokumente in das ODF Format zu tauschen.

d) *iPhone Update, jetzt aber!*[4]

Der Spiegel berichtet über eine neue Angriffsmethode betreffend iPhones. Eine Schatten-Attacke raubt das ganze Handy aus. Der iPhone-Angriff sorgt für Aufsehen. Die Sicherheitsfirma Lookout hat mit DarkSword eine hochentwickelte Exploit-Kette entdeckt, die iPhones gezielt kompromittiert und dabei in Minuten nahezu sämtliche Daten ausliest, von Passwörtern über Chats und gespeicherte Telefonnummern bis hin zu Krypto-Wallets und WLAN-Passwörtern. Angriffe konnten bis November 2025 zurückverfolgt werden. Der Exploit nutzt die Sicherheitslücken sofort aus, sobald das Gerät die präparierte Webseite oder den Schadcode lädt und extrahiert Daten in wenigen Minuten. Danach wird der Exploit nicht dauerhaft auf dem Gerät sichtbar, sodass eine Infektion schwer zu erkennen ist. Betroffen sind laut den Experten in diesem Fall nur iPhones mit den iOS-Versionen 18.4 bis 18.7, also ältere Varianten. Deshalb:

- ✔ iOS regelmäßig aktualisieren
- ✔ Vorsicht bei unbekannten Webseiten
- ✔ Sicherheitsfunktion (z. B. den Blockierungsmodus) aktivieren

Bei Bedarf, einfach mal sprechen!

1 *Quelle: techzeitgeist.de: „Instagram beendet verschlüsselte DMs ab 8. Mai“*
Quelle: theverge.com: „Instagram is getting rid of end-to-end encrypted DMs that ‘very few’ people used“
2 *Quelle: Netzpolitik.org: „Österreichische Datenschutzbehörde: Microsoft hat illegal Minderjährige getrackt“*
3 *Quelle: IT-Administrator: „Öffentliche Verwaltung steigt auf ODF um“*
4 *Quelle: SPIEGEL Netzwelt: „Warum iPhone-Nutzer jetzt Updates einspielen sollten“*