Juli 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) Integrität (Datenschutz mit Sicherheit)

(1) Ziel:

Integrität in der IT garantiert, dass Daten und Systeme vollständig, korrekt und unverändert sind. Sie stellt sicher, dass Informationen weder versehentlich noch vorsätzlich (z. B. durch Cyberangriffe, Systemfehler oder Bedienfehler) unbefugt modifiziert oder gelöscht werden können.

(2) Rechtliche Anforderung:

(2.1) Sicherheit & Richtigkeit

Nach den Grundsätzen für die Verarbeitung personenbezogener Daten in Art.5 DS-GVO ist nach Abs.1f) eine angemessene Sicherheit, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung und Schädigung durch geeignete

technische und organisatorische Maßnahmen zu gewährleisten.

(2.2) Sicherheitsanforderungen

Nach Art.32 Abs.1b) DS-GVO ist 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 mit der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

(2.3) Profiling / Fehler /Diskriminierung

Zitat aus Erwägungsgrund (71) DS-GVO in Verbindung mit Art.22 DS-GVO: Die betroffene Person sollte das Recht haben, keiner Entscheidung - was eine Maßnahme einschließen kann - zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen.

(2.4) Meldepflichten

Nach Art.33 DS-GVO sind Verletzungen des Schutzes personenbezogener Daten der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden nach Kenntnis der Verantwortlich zu melden. Nur wenn keine Risiko für die betroffenen Personen besteht kann auf die Meldung verzichtet werden. Die Mindestanforderungen sind in Abs.3 beschrieben.

Nach Art.34 DS-GVO sind bei voraussichtlich hohem Risiko für die Betroffenen diese unverzüglich über die Schutzverletzung in einfacher und klarer Sprache mit den Mindestanforderungen aus Art.33 DS-GVO zu informieren. Ausnahmen und die Art und Weise sind in Abs. 3 geregelt.

(3) Praktische Anforderungen:

(3.1) Berechtigungskonzept

Erstellung eines Berechtigungskonzeptes zur Eingrenzung von Lese- und Schreibrechten auf die jeweils benötigten Daten (Need-To-Know Prinzip).

(3.2) Signaturen

Einsatz von digitalen Signaturen zur Sicherung der Urheberschaft und der Unverfälschtheit.

(3.3) Verschlüsselung

Das Erkennen nachträglicher Änderungen an Dateien durch Hashwerte & Prüfsummen mittels eines Krypto- bzw. Verschlüsselungskonzeptes.

(3.4) IT-System härten

„Härten“ oder Absichern des IT-Systems gegen Angriffe nach dem Prinzip „Alles ist verboten, was nicht ausdrücklich erlaubt ist“. Bedeutet u. a. entfernen unnötiger Komponenten und Software, Deaktivierung ungenutzter Netzwerkverbindungen und Schnittstellen (Ports schließen), Änderung der Standardkonfiguration von Benutzernamen und Passwörtern, Konsequentes Einspielen aller Sicherheitsupdates für Betriebssystem und Anwendungen.

(3.5) Informationspflichten

Konzept zu den Informationspflichten bei Schutzverletzungen und weiteren Informationspflichten durch Erhebung aus anderen Quellen (z. B. Auskunftei), oder der Einholung von Einwilligungen bei Zweckänderung der ursprünglich erhobenen Daten

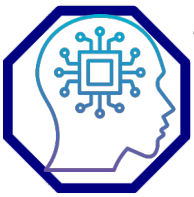
(3.6) Fazit:

Wer sich einmal Gedanken dazu gemacht hat und diese dokumentiert hat in der Regel lange Zeit „Ruhe“. Die DS-GVO verlangt keinen perfekten, unbezahlbaren Schutz, sondern ein angemessenes Schutzniveau. Was angemessen ist, ist anhand der vier Faktoren abzuwägen:

- Der Stand der Technik: Man muss aktuelle Sicherheitsstandards nutzen (z. B. keine veralteten Verschlüsselungstechniken).
- Die Implementierungskosten: Der finanzielle Aufwand muss für die Organisation leistbar und verhältnismäßig sein.
- Art, Umfang und Zweck der Verarbeitung: Ein kleines Handwerksunternehmen muss weniger Aufwand betreiben als ein Krankenhaus, das hochsensible Gesundheitsdaten speichert.
- Das Risiko für die betroffenen Personen: Wie schlimm wäre es für die Betroffenen, wenn die Daten gestohlen oder gelöscht würden?

Die Systeme sind nach modernen Standards abzusichern und es gilt für alle im Unternehmen klare Regeln dafür aufzustellen. Wie viel Geld und Mühe zu investieren ist, hängt von der Qualität bzw. der Sensibilität der Daten ab, die verarbeitet werden.

3. Am Rande notiert



a) 3x Künstliche Intelligenz im Fokus

(1.1) Gefährlich für die Öffentlichkeit

Anthropic hat mit Mythos ein neues KI-Modell vorgestellt, das so gefährlich sein soll, dass es nicht öffentlich gemacht werden soll. Stattdessen soll Claude Mythos Preview im Rahmen einer Initiative namens Project Glasswing zuerst ausschließlich einer Reihe von Firmen zur Verfügung gestellt werden, die an IT-Sicherheit arbeiten.[1]

(1.2) Sperre für Drittländer

KI-Modelle, die von einem Tag auf den anderen gesperrt werden müssen - das Vorgehen der US-Regierung bei Anthropic hat weltweit Verunsicherung ausgelöst. Es könnte weitreichende Konsequenzen haben.[2] Trumps schärfste Waffe gegen uns ist ein Exportstopp.[3]

(1.3) KI führt Cyberangriff eigenständig durch

Nach OpenAI meldet auch Anthropic Sicherheitsprobleme: Drei Claude-Modelle griffen während Tests auf externe Systeme zu. Betroffen war auch eines der leistungsstärksten Systeme des Unternehmens.[4]

b) Dual-Use-Problem: Künstliche Intelligenz

Das Fazit zu Cyberangriffen durch KI-Modelle lässt sich in eine Formel fassen: KI hat das Wettrüsten in der IT-Sicherheit dramatisch beschleunigt. Sie verändert nicht zwangsläufig die zugrundeliegenden Schwachstellen, wohl aber die Geschwindigkeit, Skalierung und Zugänglichkeit von Angriffen.[5]

Das zweischneidiger Schwert bei der Nutzung von KI: Offensive Nutzung (Angreifer) vs. Defensive Nutzung (Verteidiger); Malware Erstellung vs. Echtzeiterkennung; Täuschend echte Deepfakes und Social Engineering vs. Automatische Analyse und Filterung generiert Inhalte.

Bei Bedarf, einfach mal sprechen!

1 Quelle: heise.de: „Anthropics neues KI-Modell Mythos: Zu gefährlich für die Öffentlichkeit“
2 Quelle: tagesschau.de: „Was die Sperre für die KI-Industrie bedeutet“ und mehr
3 Quelle: focus.de: „KI und andere Technologien: Trumps schärfste Waffe gegen uns ist ein Exportstopp“
4 Quelle. Euronews.com: „Nach OpenAI nun Anthropic: KI-Modelle griffen bei Tests auf externe Systeme zu“
5 Quelle: digitalbusiness-magazin.de. „Cyberangriff durch KI: Wie sich Unternehmen jetzt aufstellen müssen“