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) „Datenminimierung“ im Datenschutz[1]

(1) Ziel:

Ziel ist die Verarbeitung und Speicherung von den Daten und nur diese Daten, die notwendiger-

1 Quelle: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html

weise für den Zeitraum der Erfüllung der getroffene Vereinbarung erforderlich sind. Das Minimierungsgebot erstreckt sich nicht nur auf die Menge der verarbeiteten Daten, sondern auch auf den Umfang der Verarbeitungen, die Speicherfristen und die Zugänglichkeit (je weniger und je kürzer, desto besser).

(2) Rechtliche Anforderungen:

(2.1) Art.5 Abs.1b und e DS-GVO – Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbeszogene Daten müssen

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; 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");

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden ("Speicherbegrenzung")

(2.2) Art.25 Abs.2 DSGVO - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

(2) Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

(3) Praktische Anforderung:

(3.1) Menge der Datenerhebung

Bei Datenerhebung sollte feststehen, welche Daten sind für diese Vereinbarung wirklich notwendig und welche Daten dienen lediglich dem Komfort und werden auf freiwilliger Basis gegeben (datenschutzfreundliche Voreinstellung). Bei einem Newsletter ist lediglich die Mailadresse und ggf. freiwillig z. B. der Name für eine persönliche Ansprache notwendig. Bei vertraglichen Vereinbarung sind alleine zur Authentifizierung mehr persönliche Daten erforderlich.

(3.2) Verarbeitung und Speicherung

Zunächst ist sicherzustellen, dass auf die gespeicherten Daten der Zugriff für eine Verarbeitung nur zu dem erhobenen Zweck erfolgt und die Daten dem Betroffenen zugänglich sind. Dazu gehört im übrigen auch der Schutz vor Zugriffe durch Dritte, auch durch Auftragsverarbeiter (z. B. Buchhaltung, Steuern u. ä.), sofern der Betroffene nicht zugestimmt hat.

(3.3) Speicher- oder Löschfrist

Mit Kündigung eines Newsletters durch den Betroffenen hat sich der Zweck der Erhebung seiner Daten erledigt und diese sind zu löschen (!). Wird ein Vertrag gekündigt, können gesetzliche Regelung gegen eine vollständige Löschung der Daten sprechen, wie Steuergesetze (Aufbewahrungsfrist zwischen 6 und 10 Jahren). Die Aufbewahrung beschränkt sich dann auf diesen Zweck, ein anderweitige Verarbeitung, z. B. für Marketingzwecke ist ohne Zustimmung des Betroffenen nicht erlaubt (eingeschränkte Verwendung oder auch zweckgebundene Verwendung). Am Ende der Aufbewahrungsfrist sind auch diese zu löschen.

(3.4) Beispiele zu Verstößen

Ausgewählte Bußgelder vom DS-GVO – Portal – Geldbußen für DS-GVO – Verstöße[2]

€ 35.000,00	Crowd Entertainment Ltd.	Versand von Werbe-SMS ohne Kundeneinwilligung
€ 400.000,00	UNICAJA BANCO	Mangelhafter Schutz von Zugriffsberechtigungen
€ 17.628.000,00	Intesa Sanpaolo	Unberechtigte Weitergabe von Daten an Tochtergesellschaften.

(3.5) Fazit

Es ist immer gut einen Plan zu haben, was mache ich wann und warum. Es bleibt ein einmaliger Aufwand sich zum Datenschutz Gedanken zu machen. Da Verzeichnis der Verarbeitungstätigkeiten in seine formfreien Anwendung ist da Hilfestellung und kein Ballast. Eine Notwendigkeit der Anpassung ist nur bei Änderungen erforderlich, dazu muss man sich eh Gedanken machen 😉.

3. Am Rande notiert

a) Neue Kreditfalle[3]

Das Postident-Verfahren schafft eigentlich ein sicheres Gefühl, dient es doch oft dazu einen fernmündlichen Vertrag rechtsverbindlich mit Sicherheit zu unterzeichnen. Das Verfahren ist auch sicher, allerdings nutzen Betrüger es aus um mit fremden Identitäten Kredite aufzunehmen und die Zahlung daraus freizugeben. Die „klassischen“ Schutzmaßnahmen sind:

- **Auftraggeber prüfen**, auf dem Papier, dem Post-Paid oder der Post-App. Bei unbekannten Namen, fremden Unternehmen oder Bank den Vorgang sofort abbrechen
- **Vorgang selbst ausgelöst**, nur dann sollten eine Ident-Verfahren gestartet werden, z. B. für die Eröffnung IHRES neuen Bankkontos, oder dem Versicherungsabschluss – Online.
- **Nie unter Zeitdruck** setzen lassen, anderenfalls versuchen Betrüger Sie damit unvorsichtig zu machen.
- **Vertrauen sie dem Empfänger**, nie PIN, TAN, Passwörter u. ä. an Dritte weitergeben. Nur Anwendungen aus sicheren Quellen nutzen.
- Im Verdachtsfall, Vorgang sofort stoppen, mögliche Schadensbeteiligte sofort informieren und in jedem Fall umgehend Anzeige bei der Polizei erstatten.

b) Die gefährlichen Altgeräte[4]

Neues Smartphone, Tablett, Notebook oder PC? Alle Daten auf dem Altgerät, löschen, überschreiben und auf Werkseinstellungen zurücksetzten! Reicht das?

Leider nicht ganz, denn die Altgeräte (mit Ihrer Hardwarekennung) bleiben ja als vertrauenswürdige Geräte auf den Plattformen erhalten und könnten durch Hacker genutzt werden. Deshalb:

- Ein Blick in die Sicherheitseinstellungen bei Google / Android, Apple und Microsoft auf die Geräteliste hilft. Nicht mehr genutzte oder verkaufte Altgeräte, wie unbekannte Geräte am besten direkt löschen.
- Taucht in der Liste ein Gerät auf, dass nicht zugeordnet werden kann, wäre aus Vorsicht ein neues Passwort für das Portal angebracht.

Bei Bedarf, einfach mal sprechen!

2 Quelle: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/
3 Quelle: t3n: „Neue Kreditfalle: So missbrauchen Betrüger das Postident-Verfahren“
4 Quelle. PC-WELT: „So gefährlich sind alte Geräte – entfernen Sie diese unbedingt aus Ihren Konten“