Februar 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) „Transparenz“ im Datenschutz

(1) Ziel:

In unterschiedlichem Maße müssen Betroffene, Betreiber von Systemen und Kontrollinstanzen erkennen können, welche Daten wann, für welchen Zweck erhoben, verarbeitet werden, welche Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung in den einzelnen Phasen besitzt. Transparenz von der Entstehung bis zur Löschung.

(2) Rechtliche Anforderung:

(2.1) Einwilligungsmanagement

Der Begriff wird in Art.4 Nr. 11 DSGVO wie folgt erläutert:

> *"Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.*

In Art.7 DSGVO werden die Bedingungen für die Einwilligung definiert und in Art.8 DSGVO für Jugendliche und Kinder bis 16 Jahre. Die Schwerpunkte sind Nachweisbarkeit, einfache, klare und verständliche Sprache, erkennbar, leichter Zugang und abgegrenzt von anderen Themenbereichen (z. B. in Abos, Verträgen u. ä.), sowie jederzeitige Möglichkeit des einfachen Widerrufs.

(2.2) Transparenz für den Betroffenen

In Art.5 DSGVO über die Grundsätze für die Verarbeitung personenbezogener Daten ist in bezeichnenderweise festgehalten:

> *Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz") … Der Verantwortliche ist für die Einhaltung … verantwortlich und muss dessen Einhaltung nachweisen können.*

In den Art. 12 – 15 DSGVO werden die erforderlichen Handlungen für die Verantwortlichen konkretisiert. Die Schwerpunkte sind transparente Informationspflichten zu Kommunikation, Rechten und einzuhaltende Fristen.

(2.3) Rechenschaft- und Nachweispflicht

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche dies nachweisen können (freiwillig, getrennt, verständlich u. a. (Nachweispflicht Art.7 DSGVO). Der Rahmen dieser Nachweispflicht wird in Art.30 DSGVO zu einem Verzeichnis der Verarbeitungstätigkeiten vorgegeben. Neben den zuvor genannten Punkten, ist die Meldung von Schutzverletzungen und deren Risikobeurteilung (Art.33-35 DSGVO), die den Umständen angemessenen technischen und organisatorischen Maßnahmen (Art.24 DSGVO) und die Zusammenarbeit mit Auftragsverarbeitern (Art.28, 29 DSGVO) anzuführen.

(3) Praktische Anforderungen:

Über alles wird eine Inventur gemacht, selbst über eingekaufte Hardware und Software, meist aber nur aus den steuerlichen Gründen der Abschreibungsmöglichkeiten. Warum nicht auch mal eine Inventur (meistens reicht 1x aus) zur Notwendigkeit, dem Zusammenspiel, der Festlegung von Abläufen (auch von selten vorkommenden Abläufen, wie z. B. Schutzverletzung) und der Effizienz dieser Anschaffungen. Bei dieser Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten sind z. B. folgende Fragen unter anderen aufgetaucht:

- Wofür haben wir verschiedene Anwendungen für den gleichen Vorgang im Einsatz?
- Wieso haben wir 2 Cloud - Anbieter im Einsatz, obwohl einer zusammen günstiger wäre?
- Hat jemand mal den IT-Support (Anbieter) gefragt, ob (mindestens) die Standards zur IT - Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik eingehalten sind?
- Gibt es einen Notfallplan? Was muss wer bei einem Schaden oder IT-Ausfall zwingend tun und wer muss dringend darüber informiert werden?
- Und es ergeben sich meist weitere Fragen, die mir über den Weg gelaufen sind.

Die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten ist ein guter Anlass dafür, zumal es keinen Formvorschriften unterliegt. Eine Schritt für Schritt Anleitung findet sich hier: „Ein einfacher Weg in 6 Schritten“. Wie beschrieben sollten man sich für die einzelnen Schritte auch Zeit

lassen. Ein Zusammenführung zu einem Verzeichnis der Verarbeitungstätigkeit ist erst am Ende notwendig. Danach ist es nur bei Veränderungen anzupassen.

3. Am Rande notiert

a) Hacker Massenangriff auf Amazon[1]

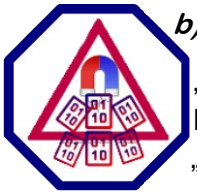
Cyberangriffe wirken oft wie “Magie”, viele Unternehmen scheitern aber an den Grundlagen, öffentlich erreichbare Administrator Ports, schwache Passwörter, keine Multi Faktor Authentifizierung. Das zeigt eine Analyse von Amazon Threat Intelligence, bei der zwischen Januar und Februar 2026 mehr als 600 FortiGate Firewalls in über 55 Ländern kompromittiert wurden, nicht über neue Zero Days, sondern über offen erreichbare Verwaltungszugänge. Neu ist vor allem der Beschleuniger, kommerzielle KI Dienste machen Planung, Skripte und Auswertung so leicht, dass auch wenig erfahrene Täter Angriffe im großen Maßstab umsetzen können.

Der Fall zeigt deutlich: KI wirkt als Beschleuniger, ersetzt aber keine fehlenden Sicherheitsmaßnahmen. Experten raten, Verwaltungszugänge nicht öffentlich erreichbar zu machen, Passwörter konsequent zu erneuern und Mehrfaktor-Authentifizierung einzusetzen. Ebenso wichtig sind Netzwerksegmentierung, aktuelle Patches und eine Überwachung auf verdächtige Aktivitäten nach einem möglichen Eindringen.

Das **BSI schreibt im IT-Grundschutz (Baustein Firewall) deshalb ausdrücklich**[2], dass Administrations- und Managementzugänge auf einzelne Quell-IP-Adressen beziehungsweise Adressbereiche zu beschränken sind und aus nicht vertrauenswürdigen Netzen kein Zugriff möglich sein darf. Für Administratoren heißt dies: Management-Ports sollten nicht öffentlich sein, Zugriff sollte nur über VPN/Jump-Host erfolgen, IP-Allowlisting und MFA sollten kontrolliert werden – genau diese Maßnahmen verhindern die hier beschriebene Angriffsklasse am zuverlässigsten.

PS: Als Datenschutzbeauftragter (DSB) würde ich mich jetzt an den Informationssicherheitsbeauftragten (ISB) oder den IT-Anbieter wenden, um die „Angelegenheit“ klären. 😉

PPS: Da hätte natürlich die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten viel Hilfestellung schon im Vorfeld gegeben. 😇



b) Fremdgesteuerte Handys durch Banking-App?

„Nein, Banking-Apps sind nicht unsicher, wenn man das Original von einer sicheren Seite herunterlädt.“ Wie ruhr24.de berichtet, warnen Experten vor fremdgesteuerten Handys: „Banking-App“ bloß nicht herunterladen“[3]. Auszug aus dem Artikel:

> *Dortmund – Das slowakische IT-Sicherheitsunternehmen ESET hat eine neue Malware entdeckt. Die Schadsoftware trägt den Namen „PromptSpy“ und tarnt sich als Banking-App namens „MorganArg“ – eine Fälschung der offiziellen Chase/JPMorgan-Banking-App. Kriminelle verbreiten sie über gefälschte Webseiten. Was macht die Anwendung so gefährlich?*

Wenn das mit Chase/JPMorgan funktioniert, kann es auch auf andere Banking-Apps bestimmt übertragen werden. Auch hier, KI ist nur ein Beschleuniger, den Betrug gab es schon vorher, d. h. Apps immer nur von einer „persönlich bekannten“, vertrauenswürdigen Quelle laden.

Bei Bedarf, einfach mal sprechen!

1 Quelle: Netzwelt.de: „Hackerangriff auf Amazon: Sind eure Kundendaten jetzt in Gefahr?“
2 Quelle: BSI IT-Grundschutzkompendium NET.3.2. Firewall“
3 Quelle: Ruhr24.de: „Experten warnen vor fremdgesteuerten Handys: „Banking-App“ bloß nicht runter laden“