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.

HINWEISE:

Das Inhaltsverzeichnis finden Sie ab Seite 2:

- ✔ Die Einzelthemen können Sie mit einem Mausklick in der Inhaltsangabe direkt ansteuern
- ✔ Mit der Suche <Strg + F> können Sie auch Ihr Thema direkt finden
- ✔ Die Quellenangaben können über einen Mausklick auf die Fußnote <NR.> direkt angesteuert werden.
- ✔ Integrierte Monatsinformationen bis: Februar 2026

1. Standard – Datenschutz – Modell Vers. 3.1a

Standard-Datenschutz-Modell *übersichtlich zusammengefasst* *11 Seiten*	**Standard-Datenschutz-Modell** Datenschutzkonferenz DSK 77 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) | Letzter Baustein 11/2021: Nr. 51 „Zugriff auf Daten, Systeme und Prozesse regeln“

**) Mit dem SDM wird im Wesentlichen die Prüfroutine für eine Datenschutzprüfung anschaulicher und detaillierter erläutert. Die Zusammenfassung des SDM auf 11 Seiten ist auf die aktuelle Version angepasst. Anspruch mit der Ergänzung ist eine verständliche und anschauliche Standardanleitung zur Planung, Umsetzung und regelmäßigen (Über-) Prüfung für die Verantwortlichen. In Folge auch für die Datenschutzbeauftragten und Aufsichtsbehörden, möglichst sogar europaweit (so der Ansatz).*

Inhalt

2. Datenschutz und Datensicherheit

a) Wofür steht DSB und ISB?

Da mich dazu immer wieder Fragestellungen erreichen, hier ein kurze Schilderung, welche Gemeinsamkeiten haben der Datenschutzbeauftragte (DSB) und der Informationssicherheitsbeauftragte (ISB) und was trennt sie auf der anderen Seite?

Im Standard-Datenschutz-Modell (SDM)[1] ist in der Einleitung festgehalten, dass DSB und ISB eine gemeinsame Sprache finden müssen, um rechtliche Anforderung des Datenschutzes zur Verwendung von Daten und deren Aufbewahrung sicherzustellen. Aus Sicht des Datenschutzes ergeben sich aus den 7 Gewährleistungszielen mehrfache Überschneidungen.

(1) Datenschutz

(1.1) Transparenz

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.

(1.2) Nichtverkettung

Die Vermeidung einer Zusammenführung / Verkettung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, ist durch technische und organisatorische Maßnehmen sicherzustellen (Pseudonymisierung, Anonymisierung, Berechtigungskonzepte). Eine rechtliche zu-lässige Verkettung ist nur unter eng definierten Umständen möglich.

(1.3) Datenminimierung

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).

(1.4) Intervenierbarkeit

Erfüllung der den Betroffenen zustehenden Rechten auf Benachrichtigung, Auskunft, Berichtigung, Löschung, Einschränkung, Übertragbarkeit, Widerspruch und Eingriff in automatisierte Bewertungs- und Entscheidungsprozesse, Profiling, sowie Maßnahmen zur Identifizierung bzw. Authentisierung. Zwecks Erfüllung der Betroffenenrechte und möglichen, behördlichen Anordnungen muss der Verantwortliche jederzeit Eingriff in die Prozesse nehmen können.

(2) Datenschutz und Datensicherheit

(2.1) Vertraulichkeit

Kein Zugriff, Kenntnisnahme oder Nutzung der Daten durch unbefugte Dritte, ob externe, Beschäftigte oder alle Arten von Dienstleistern. Dies gilt auch bei allen Arten von Zwischenfällen.

(2.2) Integrität

Sicherstellung der technischen Prozesse und Systeme in Bezug auf die kontinuierliche Einhaltung der festgelegten Spezifikationen, sowie der Erhalt der Vollständigkeit, Richtigkeit, Unversehrtheit und Aktualität der Daten. Angemessene und regelmäßige Überwachung der Einhaltung, um Abweichungen festzustellen und anzupassen, wo es erforderlich ist. Neben der Fehlerfreiheit ist die Diskriminierungsfreiheit bei automatisierten Bewertungs- und Entscheidungsprozessen IM VORFELD zu prüfen, festzulegen und im Prozess sicherzustellen.

1 *Quelle: Datenschutzkonferenz der Länder DSK: „Standard Datenschutz Modell“*

(2.3) *Verfügbarkeit*

Unverzüglicher Zugriff auf und Auffindbarkeit der (personenbezogenen) Daten und der Verarbeitung im ordnungsgemäß vorgesehenen Prozess, einschließlich einer angemessenen, gut verständlichen Darstellung für die Person (Datenmanagement – Systeme, Datenbanken, Suchfunktionen). Ein Schutz und zügiger Zugriff auch bei physischen oder technischen Zwischenfällen und bei hoher Systemlast. Bei Ausnahme eines Störfalles sind und werden Maßnahmen zur Behebung getroffen.

(3) Datenschutzbeauftragte[2]:

(3.1) *Aufgaben*

Ein Datenschutzbeauftragter überwacht und unterstützt die Einhaltung der Datenschutzgesetze im Unternehmen. Seine Tätigkeit umfasst unter anderem:

- Beratung der Geschäftsführung und Mitarbeitenden zu Datenschutzfragen.
- Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften.
- Prüfung und Dokumentation von Datenverarbeitungsprozessen.
- Durchführung oder Koordination von Schulungen zum Datenschutz.
- Ansprechpartner für Betroffene und Aufsichtsbehörden.
- Meldung und Bewertung von Datenschutzvorfällen.

Der Fokus liegt auf dem Schutz personenbezogener Daten und der Wahrung der Rechte der Betroffenen. Aufsichtsbehörde: BfDI – Bundesbeauftragte/r für den Datenschutz und die Informationsfreiheit und deren Vertretern in den Ländern.

(3.2) *Erforderlichkeit*

Ein Datenschutzbeauftragter lohnt sich spätestens, wenn die gesetzlichen Schwellen erreicht oder sensible Daten verarbeitet werden. Oft lohnt er sich aber schon früher, weil er Risiken minimiert, Prozesse sauber aufsetzt und Vertrauen schafft. 😉

(4) Informationssicherheitsbeauftragte[3]:

(4.1) *Aufgaben*

Ein Informationssicherheitsbeauftragter ist für die Sicherheit aller Informationen im Unternehmen verantwortlich – unabhängig davon, ob personenbezogen oder nicht. Seine Aufgaben beinhalten:

- Aufbau, Pflege und Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS).
- Analyse von Risiken für IT-Systeme und Geschäftsprozesse.
- Definition und Überwachung von Sicherheitsmaßnahmen (technisch und organisatorisch).
- Sensibilisierung und Schulung der Mitarbeitenden zur Informationssicherheit.
- Koordination bei Sicherheitsvorfällen und Unterstützung im Incident Management.
- Beratung der Unternehmensleitung zu Sicherheitsstrategien.

Der Fokus liegt auf Vertraulichkeit, Integrität und Verfügbarkeit aller Unternehmensinformationen. Aufsichtsbehörde: BSI – Bundesamt für Sicherheit in der Informationstechnik.

(4.2) *Erforderlichkeit*

Ein Informationssicherheitsbeauftragter lohnt sich spätestens, wenn ein ISMS (Informations-Sicherheits-Management-System eingeführt, NIS-2-Pflichten zu erfüllen sind oder ein erhöhtes Cyberrisiko besteht. In der Praxis setzen viele Unternehmen bereits früher auf einen ISB, um Haftungsrisiken zu reduzieren, Prozesse zu professionalisieren und Angriffe zu verhindern.

b) „Transparenz“ im Datenschutz

(1) Ziel:

In unterschiedlichem Maße müssen Betroffene, Betreiber von Systemen und Kontrollinstanzen

2 Quelle: Management-Info zum Standard-Datenschutz-Modell
3 Quelle: Management-Info BSI / IT Grundschutz Basiswissen

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

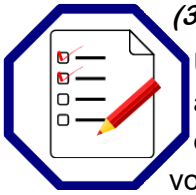
In Art.5 DSGVO über die Grundsätze für die Verarbeitung personenbezogener Daten ist in bezeichnenderweise festgehalten:

> *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) Die kleinen Helfer im digitalen Alltag

Das Bundesamt für die Sicherheit in der Informationstechnik hat unter „Wegweiser im digitalen Alltag“[4] nützliche und kurzweilige Informationsbroschüren veröffentlicht. Themen sind unter anderen Checkliste für den Ernstfall: Gehackter Account, Wegweiser kompakt: Tipps für mehr E-Mail-Sicherheit, Checkliste für den Ernstfall: Phishing, Checkliste für den Ernstfall: Betrug beim Onlinebanking und weitere Themen.

Fazit: Lesenswert

b) Hacker Massenangriff auf Amazon[5]

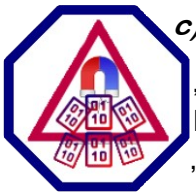
Cyberangriffe wirken oft wie “Magie”, viele Unternehmen scheitern aber an den Grundlagen, öffentlich erreichbare Administrator Ports, schwache Passwörter, keine Multi Faktor Authentifizierung. Das zeigt eine Analyse von Amazon Threat Intelligence, bei der zwischen Januar und Februar 2026 mehr als 600 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**[6], 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. 😇



c) 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“[7]. 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?

4 Quelle: BSI „Wegweiser im digitalen Alltag“
5 Quelle: Netzwelt.de: „Hackerangriff auf Amazon: Sind eure Kundendaten jetzt in Gefahr?“
6 Quelle: BSI IT-Grundschutzkompendium NET.3.2. Firewall“
7 Quelle: Ruhr24.de: „Experten warnen vor fremdgesteuerten Handys: „Banking-App“ bloß nicht runter laden“

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!