



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.

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.

Inhalt

(Einfach interessantes Thema nach Wahl anklicken)

1. Standard – Datenschutz – Modell Vers. 3.1a...1	(2.4) Weitere Einwirkungsrechte.....2
2. Datenschutz und Datensicherheit.....1	(2.5) Und nicht zu vergessen:.....2
✗ a) Intervenierbarkeit im Datenschutz.....1	(3) Praktische Anforderungen.....2
(1) Ziel.....1	(3.1) „Single Point of Contact“.....2
(2) Rechtliche Anforderungen.....2	(3.2) Umfang von Maßnahmen.....2
(2.1) Art. 12 DS-GVO „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person“ unter anderem.....2	(3.3) Technische Maßnahmen u.a.....2
(2.2) Art. 5 DS-GVO „Grundsätze für die Verarbeitung personenbezogener Daten“.....2	(3.4) Organisatorische Maßnahmen u.a.....3
(2.3) Artikel zu den Rechten der Betroffenen, u.a.: 2	(4) Fazit:.....3
	✗ 3. Am Rande notiert.....3
	a) „Warum betrifft Cybersicherheit uns alle?“.....3
	b) Microsoft, das nächste Support-Ende.....3

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



Bundesdatenschutzgesetz
 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) Intervenierbarkeit im Datenschutz

(1) Ziel

Ziel ist die 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) Rechtliche Anforderungen

(2.1) Art.12 DS-GVO „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person“ unter anderem:

- ✔ Der Verantwortliche trifft geeignete Maßnahmen, um betroffenen Personen präzise, transparent, verständlich, leicht zugänglich und in einfacher und klarer Sprache alle Informationen und Mitteilungen zur Verarbeitung zu übermitteln.
- ✔ Der Verantwortliche erleichtert betroffenen Personen ihre Recht unentgeltlich auszuüben. Anfragen der Betroffenen sind unverzüglich, spätestens nach 30 Tage zu beantworten. Gut begründete Verzögerungen (z.B. mangelnde Identitätsbestimmung) sind ebenfalls in dieser Frist mitzuteilen, mit deutlichem Hinweis auf die Möglichkeit der Beschwerde bei der zuständigen Aufsichtsbehörde.

(2.2) Art.5 DS-GVO „Grundsätze für die Verarbeitung personenbezogener Daten“

Die Grundsätze der Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit das Fundament für die Verarbeitung personenbezogener Daten. Der Verantwortliche dazu verpflichtet, die Einhaltung dieser Prinzipien lückenlos nachzuweisen.

(2.3) Artikel zu den Rechten der Betroffenen, u.a.:

- ▶ [Art.16 DS-GVO](#) Recht auf Berichtigung
- ▶ [Art.17 DS-GVO](#) Recht auf Löschung / Vergessen werden
- ▶ [Art.18 DS-GVO](#) Recht auf Einschränkung der Verarbeitungen
- ▶ [Art.20 DS-GVO](#) Recht auf Datenübertragbarkeit (wieder-, ein-, lesbarer Form)
- ▶ [Art.22 DS-GVO](#) Rechte bei automatisierten Entscheidungen, einschließlich Profiling

(2.4) Weitere Einwirkungsrechte

- ▣ [Art.33 DS-GVO](#) „Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde“ i. V. m. Art.34 DS-GVO „Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person“.
- ▣ [Art.58 DS-GVO](#) „Befugnisse der Aufsichtsbehörde“,

(2.5) Und nicht zu vergessen:

- ✔ [Art.7 Abs.3 DS-GVO](#) „Bedingungen für die Einwilligung“ jederzeitiges Widerrufsrecht [Art.25 DS-GVO](#) als Verpflichtung zu einer datenschutzfreundlichen Voreinstellung.

(3) Praktische Anforderungen

(3.1) „Single Point of Contact“

Zur Ausübung der Rechte durch die Betroffenen sollte es bei allen Kommunikationsformen (Web, Telefon, Gespräch, Vertrag) einen einfach zu findenden zentralen „Anlaufpunkt“ geben, um ihre Rechte einfach und wirksam durchsetzen zu können.

(3.2) Umfang von Maßnahmen

Wie in Art.25 Abs.1 DS-GVO ausgeführt hängt es von Art und Größenordnung ab, denn:

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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen

(3.3) Technische Maßnahmen u.a.

- ✔ Zentrale Steuerung: Einrichtung von Schnittstellen (APIs) zur sofortigen Systemsperrung.
- ✔ Modulare Löschkonzepte: Daten müssen feingranular löscherbar sein, ohne Systemabstürze zu verursachen.

- ❖ Export-Funktionen: Automatisierte Bereitstellung aller Daten in maschinenlesbaren Formaten (z. B. JSON).
- ❖ Status-Flags: Kennzeichnung von Datenfeldern bei Widerspruch oder Richtigkeitsprozessen.
- ❖ Sperrmechanismen: Temporäre Ausblendung von Datensätzen bei laufenden Prüfungen.



(3.4) Organisatorische Maßnahmen u.a.

- ❖ Einfache Kanäle: Bereitstellung von Webformularen oder Self-Service-Portalen für Betroffene.
- ❖ Klare Prozesse: Festgelegte Zuständigkeiten für die Bearbeitung von Löschanfragen.
- ❖ Fristen-Monitoring: Automatische Erinnerungen zur Einhaltung der gesetzlichen 1-Monats-Frist.
- ❖ Mitarbeiter-Schulung: Regelmäßiges Training des Supports zum Erkennen von Betroffenenanfragen.
- ❖ Dienstleister-Steuerung: Vertragliche Pflichten zur Datenlöschung bei Subunternehmern (Auftragsverarbeitung).



(4) **Fazit:**

Die immer gewünschte hohe Datenqualität kann nur mit dem Nutzer und möglichst über eine einfache Korrekturfunktion erreicht werden. Eine Prozessautomatisierung durch Self - Service Anwendungen reduziert den IT-Aufwand, die Kosten für Support und erleichtert eine spätere Migration durch standardisierte Export- und Löschroutinen. Nebenbei werden die Haftungsrisiken reduziert, das Risiko vor Sanktionen / Bußgeldern durch die Aufsichtsbehörden minimiert und die vorgegeben Fristen werden möglichst eingehalten.

Die Intervenierbarkeit stärkt dabei vor allem das Vertrauen der Kunden.

3. Am Rande notiert



a) „Warum betrifft Cybersicherheit uns alle?“

Aus dem Beitrag der tagesschau vom 27.05.2026 zitiert:

Viele Menschen glauben noch immer, ihr Handy oder ihr Computer seien für Kriminelle nicht interessant und gehen beim Schutz entsprechend nachlässig vor. Dabei reicht oft schon ein schwaches Passwort oder ein unbedachter Klick, damit Angreifer Zugriff auf Daten oder Konten bekommen. Cyberangriffe treffen aber nicht nur Privatpersonen, sondern auch große Konzerne, staatliche Institutionen, Flughäfen, Schulen, Kommunen und mittelständische Unternehmen. Hinter den Attacken von Cyberbanden mit Namen wie "Lockbit" oder "Badbox" stehen meist finanzielle Interessen, der Diebstahl sensibler Daten, Spionage oder gezielte Erpressung.



b) Microsoft, das nächste Support-Ende²

Microsoft beendet die Unterstützung für Office 2021 zum 13. Oktober 2026, d. h.

- *Microsoft bietet keinen technischen Support, Fehlerbehebungen oder Sicherheitsbehebungen mehr für Schwachstellen von Office 2021, die später gemeldet oder entdeckt werden können. Dazu gehören Sicherheitsupdates, die Ihren PC vor schädlichen Viren, Spyware und anderer bösartiger Software schützen können.*
- *Sie erhalten keine Office 2021-Software-Updates mehr von Microsoft Update.*
- *Sie erhalten keinen telefonischen oder chat-technischen Support mehr.*
- *Weitere Updates für Support-Inhalte werden nicht bereitgestellt und die meisten Online-Hilfeinhalte werden eingestellt.*

Beim Support von Microsoft ist ein Terminkalender mit Erinnerungsfunktion schon sehr hilfreich! 😊

Bei Bedarf, einfach mal sprechen!

1 Quelle tagesschau.de „Cyberkriminalität“

2 Quelle Microsoft: „End of support for Office 2021 → By or Try Microsoft 365“