

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.

## 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 <<sup>NR.</sup>> direkt angesteuert werden.
- ✓ Integrierte Monatsinformationen bis: September 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



**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) | 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

|                                                                                                                           |           |
|---------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. Standard – Datenschutz – Modell Vers. 3.1a</b>                                                                      | <b>1</b>  |
| <b>2. Datenschutz und Datensicherheit</b>                                                                                 | <b>5</b>  |
| <b>a) Wofür steht DSB und ISB?</b>                                                                                        | <b>5</b>  |
| (1) <i>Datenschutz</i>                                                                                                    | 5         |
| (1.1) <i>Transparenz</i>                                                                                                  | 5         |
| (1.2) <i>Nichtverkettung</i>                                                                                              | 5         |
| (1.3) <i>Datenminimierung</i>                                                                                             | 5         |
| (1.4) <i>Intervenierbarkeit</i>                                                                                           | 5         |
| (2) <i>Datenschutz und Datensicherheit</i>                                                                                | 5         |
| (2.1) <i>Vertraulichkeit</i>                                                                                              | 5         |
| (2.2) <i>Integrität</i>                                                                                                   | 5         |
| (2.3) <i>Verfügbarkeit</i>                                                                                                | 6         |
| (3) <i>Datenschutzbeauftragte</i>                                                                                         | 6         |
| (3.1) <i>Aufgaben</i>                                                                                                     | 6         |
| (3.2) <i>Erforderlichkeit</i>                                                                                             | 6         |
| (4) <i>Informationssicherheitsbeauftragte</i>                                                                             | 6         |
| (4.1) <i>Aufgaben</i>                                                                                                     | 6         |
| (4.2) <i>Erforderlichkeit</i>                                                                                             | 6         |
| (5) <i>Fazit</i>                                                                                                          | 6         |
| <b>b) „Transparenz“ im Datenschutz</b>                                                                                    | <b>7</b>  |
| (1) <i>Ziel</i>                                                                                                           | 7         |
| (2) <i>Rechtliche Anforderung</i>                                                                                         | 7         |
| (2.1) <i>Einwilligungsmanagement</i>                                                                                      | 7         |
| (2.2) <i>Transparenz für den Betroffenen</i>                                                                              | 7         |
| (2.3) <i>Rechenschaft- und Nachweispflicht</i>                                                                            | 7         |
| (3) <i>Praktische Anforderungen</i>                                                                                       | 7         |
| (4) <i>Fazit</i>                                                                                                          | 8         |
| <b>c) „Nichtverkettung“ im Datenschutz</b>                                                                                | <b>8</b>  |
| (1) <i>Ziel</i>                                                                                                           | 8         |
| (2) <i>Rechtliche Anforderung</i>                                                                                         | 8         |
| (3) <i>Praktische Anforderungen</i>                                                                                       | 8         |
| (3.1) <i>Zweckbindung</i>                                                                                                 | 8         |
| (3.2) <i>Datentrennung</i>                                                                                                | 9         |
| (3.3) <i>Profiling</i>                                                                                                    | 9         |
| (3.4) <i>Beispiele für mögliche Verstöße</i>                                                                              | 9         |
| (4) <i>Fazit</i>                                                                                                          | 9         |
| <b>d) „Datenminimierung“ im Datenschutz</b>                                                                               | <b>9</b>  |
| (1) <i>Ziel</i>                                                                                                           | 9         |
| (2) <i>Rechtliche Anforderungen</i>                                                                                       | 9         |
| (2.1) <i>Art. 5 Abs. 1b und e DS-GVO – Grundsätze für die Verarbeitung personenbezogener Daten</i>                        | 9         |
| (2.2) <i>Art. 25 Abs. 2 DSGVO - Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen</i> | 10        |
| (3) <i>Praktische Anforderung</i>                                                                                         | 10        |
| (3.1) <i>Menge der Datenerhebung</i>                                                                                      | 10        |
| (3.2) <i>Verarbeitung und Speicherung</i>                                                                                 | 10        |
| (3.3) <i>Speicher- oder Löschfrist</i>                                                                                    | 10        |
| (3.4) <i>Ausgewählte Bußgelder - Datenminimierung</i>                                                                     | 10        |
| (4) <i>Fazit</i>                                                                                                          | 10        |
| <b>e) Intervenierbarkeit im Datenschutz</b>                                                                               | <b>10</b> |

|                                                                                                                                                       |           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| (1) Ziel.....                                                                                                                                         | 10        |
| (2) Rechtliche Anforderungen.....                                                                                                                     | 11        |
| (2.1) Art. 12 DS-GVO „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person“ unter anderem:..... | 11        |
| (2.2) Art. 5 DS-GVO „Grundsätze für die Verarbeitung personenbezogener Daten“.....                                                                    | 11        |
| (2.3) Artikel zu den Rechten der Betroffenen, u.a.:.....                                                                                              | 11        |
| (2.4) Weitere Einwirkungsrechte.....                                                                                                                  | 11        |
| (2.5) Und nicht zu vergessen:.....                                                                                                                    | 11        |
| (3) Praktische Anforderungen.....                                                                                                                     | 11        |
| (3.1) „Single Point of Contact“.....                                                                                                                  | 11        |
| (3.2) Umfang von Maßnahmen.....                                                                                                                       | 11        |
| (3.3) Technische Maßnahmen u.a.....                                                                                                                   | 12        |
| (3.4) Organisatorische Maßnahmen u.a.....                                                                                                             | 12        |
| (4) Fazit:.....                                                                                                                                       | 12        |
| <b>f) Vertraulichkeit (Datenschutz mit Sicherheit).....</b>                                                                                           | <b>12</b> |
| (1) Ziel:.....                                                                                                                                        | 12        |
| (2) Rechtliche Anforderungen:.....                                                                                                                    | 12        |
| (3) Praktische Anforderungen:.....                                                                                                                    | 13        |
| (3.1) Zugriffsbeschränkungen:.....                                                                                                                    | 13        |
| (3.2) Zugangskontrollen:.....                                                                                                                         | 13        |
| (3.3) Verschlüsselung:.....                                                                                                                           | 13        |
| (4) Fazit:.....                                                                                                                                       | 13        |
| <b>g) Integrität (Datenschutz mit Sicherheit).....</b>                                                                                                | <b>13</b> |
| (1) Ziel:.....                                                                                                                                        | 13        |
| (2) Rechtliche Anforderung:.....                                                                                                                      | 13        |
| (2.1) Sicherheit & Richtigkeit.....                                                                                                                   | 13        |
| (2.2) Sicherheitsanforderungen.....                                                                                                                   | 13        |
| (2.3) Profiling / Fehler / Diskriminierung.....                                                                                                       | 14        |
| (2.4) Meldepflichten.....                                                                                                                             | 14        |
| (3) Praktische Anforderungen:.....                                                                                                                    | 14        |
| (3.1) Berechtigungskonzept.....                                                                                                                       | 14        |
| (3.2) Signaturen.....                                                                                                                                 | 14        |
| (3.3) Verschlüsselung.....                                                                                                                            | 14        |
| (3.4) IT-System härten.....                                                                                                                           | 14        |
| (3.5) Informationspflichten.....                                                                                                                      | 14        |
| (4) Fazit:.....                                                                                                                                       | 14        |
| <b>h) Verfügbarkeit (Datenschutz mit Sicherheit).....</b>                                                                                             | <b>15</b> |
| (1) Ziel:.....                                                                                                                                        | 15        |
| (2) Rechtliche Anforderungen:.....                                                                                                                    | 15        |
| (2.1) Begrenzung.....                                                                                                                                 | 15        |
| (2.2) Sicherheit.....                                                                                                                                 | 15        |
| (2.3) Information und Auskunft.....                                                                                                                   | 15        |
| (2.4) Datenübertragung.....                                                                                                                           | 15        |
| (3) Praktische Anforderungen:.....                                                                                                                    | 15        |
| (3.1) Routine:.....                                                                                                                                   | 16        |
| (3.2) Kernkompetenzen:.....                                                                                                                           | 16        |
| (4) Fazit:.....                                                                                                                                       | 16        |
| <b>i) Wer verantwortet den Datenschutz?.....</b>                                                                                                      | <b>16</b> |
| (1) Ziel:.....                                                                                                                                        | 16        |
| (2) Rechtsgrundlage:.....                                                                                                                             | 16        |
| (3) Praktisch:.....                                                                                                                                   | 17        |
| (3.1) Verantwortlich ist:.....                                                                                                                        | 17        |
| (3.2) Nicht verantwortlich sind:.....                                                                                                                 | 17        |

|                                                              |           |
|--------------------------------------------------------------|-----------|
| (4) Mitverantwortliche im Datenschutz?                       | 17        |
| (4.1) Auftragsverarbeiter:                                   | 17        |
| (4.1.1) Definition:                                          | 17        |
| (4.1.2) Rechtsgrundlage:                                     | 17        |
| (4.1.3) Praktisch:                                           | 17        |
| (4.2) Gemeinsam Verantwortliche?                             | 18        |
| (4.2.1) Definition:                                          | 18        |
| (4.2.2) Rechtsgrundlage:                                     | 18        |
| (4.2.3) Praktisch:                                           | 18        |
| <b>3. Am Rande notiert</b>                                   | <b>18</b> |
| a) Die kleinen Helfer im digitalen Alltag                    | 18        |
| b) Hacker Massenangriff auf Amazon                           | 18        |
| c) Fremdgesteuerte Handys durch Banking-App?                 | 19        |
| d) Meta – Instagram beendet verschlüsselte Direktnachrichten | 19        |
| e) Trackt Microsoft illegal Minderjährige?                   | 19        |
| f) Microsoft Word fliegt raus!                               | 20        |
| g) iPhone Update, jetzt aber!                                | 20        |
| h) Neue Kreditfalle                                          | 20        |
| i) Die gefährlichen Altgeräte                                | 20        |
| j) „Warum betrifft Cybersicherheit uns alle?“                | 21        |
| k) Microsoft, das nächste Support-Ende                       | 21        |
| l) „Wenn der Datenschützer (ich) sauer wird!“                | 21        |
| (1.1) Umstand:                                               | 21        |
| (1.2) Fragen an die Datenschutzbeauftragten:                 | 21        |
| (1.3) Antworten:                                             | 22        |
| (1.4) Was war falsch?                                        | 22        |
| (1.5) Konzernprivileg DS-GVO ??                              | 22        |
| (1.6) Konsequenz:                                            | 22        |
| m) 3x Künstliche Intelligenz im Fokus                        | 22        |
| (1.1) Gefährlich für die Öffentlichkeit                      | 22        |
| (1.2) Sperre für Drittländer                                 | 22        |
| (1.3) KI führt Cyberangriff eigenständig durch               | 23        |
| n) Dual-Use-Problem: Künstliche Intelligenz                  | 23        |
| o) Personalausweis: Kein Pfand und Kopiereinschränkungen     | 23        |
| (1.1) Deutlicher Hinweis:                                    | 23        |
| (1.2) Warum:                                                 | 23        |
| (1.3) Dringende Empfehlung BfM:                              | 23        |
| p) Es liegt nicht am Datenschutz!                            | 24        |

## 2. Datenschutz und Datensicherheit

### a) *Wofür steht DSB und ISB?*

Da mich dazu immer wieder Fragestellungen erreichen, hier eine 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)<sup>1</sup> ist in der Einleitung festgehalten, dass DSB und ISB eine gemeinsame Sprache finden müssen, um rechtliche Anforderungen 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 Maßnahmen sicherzustellen (Pseudonymisierung, Anonymisierung, Berechtigungskonzepte). Eine rechtliche zulässige 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.

<sup>1</sup> Quelle: Datenschutzkonferenz der Länder DSK: „Standard Datenschutz Modell“



### (2.3) Verfügbarkeit

Unverzögerlicher 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<sup>2</sup>:**

#### (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<sup>3</sup>:**

#### (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 (Informationssicherheits-Management-System) eingeführt, NIS-2-Pflichten zu erfüllen sind oder ein erhöhtes Cyberisiko besteht. In der Praxis setzen viele Unternehmen bereits früher auf einen ISB, um Haftungsrisiken zu reduzieren, Prozesse zu professionalisieren und Angriffe zu verhindern.



### (5) **Fazit:**

- ✓ Datenschutzbeauftragter (DSB): Überwacht die Einhaltung von Datenschutzgesetzen, berät Mitarbeiter und Geschäftsführung beim Umgang mit Kund- oder Mitarbeiterdaten und

<sup>2</sup> Quelle: [Management-Info zum Standard-Datenschutz-Modell](#)

<sup>3</sup> Quelle: [Management-Info BSI / IT Grundsicherheits Basiswissen](#)

dokumentiert Verarbeitungsprozesse.

- ✓ Informationssicherheitsbeauftragter (ISB): Schützt das Unternehmen vor Ausfällen, Spionage oder Datenklau durch die Sicherung der Vertraulichkeit, Verfügbarkeit und Integrität aller Daten und Systeme.
- ✓ Beide Rollen ergänzen sich ideal, sollten aber wegen möglicher Interessenkonflikte (z. B. bei Überwachungsmaßnahmen am Arbeitsplatz) in der Organisation möglichst nicht von derselben Person in Personalunion ausgeübt werden.

## b) „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) Einwilligungsmangement

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

Beruhet 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.



#### (4) Fazit:

Transparenz ist das Fundament für Vertrauen und Rechtmäßigkeit. Fazit für die Praxis ist echte Transparenz gelingt heute vor allem durch nutzerfreundliche Ansätze wie mehrstufige Datenschutzerklärungen (Layered Privacy Notices) oder den Einsatz von klaren Icons. Sie verwandelt Datenschutz von einer lästigen Pflichtaufgabe in ein sichtbares Qualitätsmerkmal für ein digitales Unternehmen.



#### c) „Nichtverkettung“ im Datenschutz

##### (1) Ziel:

Die Vermeidung einer Zusammenführung (Verkettung) von Daten, die zu unterschiedlichen bzw. zu anderen Zwecken erhoben wurden (fehlender Rechtsgrund). Eine rechtliche, zulässige Verkettung ist nur unter eng definierten Umständen möglich. Dies ist durch technische und organisatorische Maßnahmen (z. B. Pseudonymisierung, Anonymisierung, Berechtigungskonzepte) sicherzustellen.



##### (2) Rechtliche Anforderung

Die rechtliche Anforderung ergibt sich aus [Art.5 Abs.1b](#) der DS-GVO über die Grundsätze für die Verarbeitung personenbezogener Daten:

(1) *Personenbezogene Daten müssen:*

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

und zu den eng definierten Umständen:

(1) b) *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");*

In [Art.89 Abs.1](#) DS-GVO geht es um Garantie für die Verarbeitung der in Art.5 Abs. 1b genannten Ausnahmen. Auszug:

*Mit diesen Garantien wird sichergestellt, dass technische und organisatorische Maßnahmen bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird.*



##### (3) Praktische Anforderungen

Anwendungen, Systeme und Berechtigungen sollten so gestaltet sein, dass nur auf personenbezogene Daten zugegriffen werden kann, für die eine Rechtsgrundlage besteht.

##### (3.1) Zweckbindung

Daten, die für einen bestimmten Zweck erhoben werden, dürfen nicht einfach mit Daten für

einen anderen Zweck kombiniert oder für einen ganz anderen Zweck genutzt werden.

(3.2) Datentrennung

Technisch und organisatorisch muss sichergestellt werden, dass Datenbestände aus unterschiedlichen Verarbeitungsprozessen getrennt bleiben.

(3.3) Profiling

Durch die Nichtverkettung ist zu verhindern, dass verschiedene Informationen aus unterschiedlichen Lebensbereichen zusammengeführt werden, was die Privatsphäre der betroffenen Personen stark beeinträchtigen könnte (Profiling ist mit weiteren Anforderungen verknüpft).

(3.4) Beispiele für mögliche Verstöße

- ▶ Erhalt von Kontaktdaten (Visitenkarte) sind keine, gleichzeitige Einwilligung in Werbung
- ▶ Und auch keine Einwilligung in der Verarbeitung / Speicherung bei oder durch Auftragsverarbeiter
- ▶ Personendaten aus erledigten und abgerechneten Verträgen sind zwar für die Finanzverwaltung nach GoBD entsprechend aufzubewahren (Rechtsgrund: Gesetz), dürfen aber nicht mehr für Werbung, Kontakt, Information u. ä verwendet werden, da dafür der Zweck entfallen ist.

(4) **Fazit:**

Zusammengefasst zielt die Nichtverkettung darauf ab, die Zweckbestimmung der Datenverarbeitung zu garantieren und die Erstellung von Persönlichkeitsprofilen durch die Zusammenführung isolierter Datenquellen zu verhindern. Für die Praxis fordert die Nichtverkettung von Unternehmen ein konsequentes „Silo-Denken“ bei der Datenverarbeitung. Auch wenn die technische Zusammenführung von Marketing-, HR- und Kundendaten oft verlockend erscheint, ist sie ohne ausdrückliche Einwilligung oder separate Rechtsgrundlage datenschutzrechtlich unzulässig. Sie zwingt dazu, Daten von vornherein isoliert und zweckgebunden zu verarbeiten.

d) „Datenminimierung“ im Datenschutz<sup>4</sup>

(1) **Ziel:**

Ziel ist die Verarbeitung und Speicherung von den Daten und nur diese Daten, die notwendigerweise 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) *Personenbezogene 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")*

<sup>4</sup> Quelle: <https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Technik/SDM.html>

Dokument von <https://volkerschroer.de>

(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 Vereinbarungen 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 Regelungen 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) Ausgewählte Bußgelder - Datenminimierung<sup>5</sup>

|                 |                          |                                                              |
|-----------------|--------------------------|--------------------------------------------------------------|
| € 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. |

(4) **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. Das Verzeichnis der Verarbeitungstätigkeiten in seiner formatfreien Anwendung ist da Hilfestellung und kein Ballast. Eine Notwendigkeit der Anpassung ist nur bei Änderungen erforderlich, dazu muss man sich eh Gedanken machen 😊.

e) 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

<sup>5</sup> Quelle: <https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/>

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 Rechte unentgeltlich auszuüben. Anfragen der Betroffenen sind unverzüglich, spätestens nach 30 Tagen 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 sind das Fundament für die Verarbeitung personenbezogener Daten. Der Verantwortliche ist dazu verpflichtet, die Einhaltung dieser Prinzipien der Verordnung 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*

men

(3.3) Technische Maßnahmen u.a.

- ◆ Zentrale Steuerung: Einrichtung von Schnittstellen (APIs) zur sofortigen Systemspernung.
- ◆ Modulare Löschkonzepte: Daten müssen feingranular löscher 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.

f) Vertraulichkeit (Datenschutz mit Sicherheit)(1) **Ziel:**

Im Datenschutz bedeutet Vertraulichkeit, dass personenbezogene Daten ausschließlich von berechtigten Personen eingesehen, verarbeitet oder weitergegeben werden. Sie garantiert, dass Unbefugte keinen Zugriff auf sensible Informationen erhalten. Dieses Schutzziel ist ein zentraler Grundsatz der Datenschutz – Grundverordnung (DS-GVO). Der Schutz vor unbefugter Offenlegung oder Datenpannen ist entscheidend, um die Privatsphäre der Betroffenen zu wahren. Ein Verlust von Vertraulichkeit – beispielsweise bei sensiblen Gesundheitsdaten oder Finanzinformationen – kann schwerwiegende Konsequenzen für die betroffene Person haben und für das verantwortliche Unternehmen zu einem enormem Vertrauensverlust führen.

(2) **Rechtliche Anforderungen:**

Art.5 Abs.1.f) DS-GVO, die Grundsätze für die Verarbeitung ...

*„in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“*

Die Auftragsverarbeiter werden über Art.28 und 29 DS-GVO in gleicher Weise eingebunden. Mit Art.32 Abs.1.b) in die Vorgaben zur Sicherheit der Verarbeitung integriert:

*(1) 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 ... b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen.*

Die Maßnahmen und Fristen bei Verletzung der Vertraulichkeit sind in [Art.33,34 DS-GVO](#) geregelt.



**(3) Praktische Anforderungen:**

**(3.1) Zugriffsbeschränkungen:**

Implementierung eines sicheren Authentifizierungsverfahrens. Regelung und Kontrolle der Nutzung zugelassener Ressourcen, Kommunikationskanäle, Abläufe und vertragliche Verpflichtungen. Festlegung von Passwortrichtlinien, komplexe Berechtigungskonzepte und Zwei-Faktor-Authentifizierung (2FA), sodass nur Zugriff auf die Daten bestehen, die für die Nutzung erforderlich sind.

**(3.2) Zugangskontrollen:**

Physischer Schutz von Servern und Akten durch beispielsweise Schließanlagen oder Sicherheitspersonal. Enge Eingrenzung des Berechtigungs- und Rollenkonzeptes auf nachprüfbares, identifiziertes und zulässiges Personal, dass örtlich, fachlich zuständig, befähigt, zuverlässig, ist, keinen Interessenkonflikten unterliegt und in angemessen ausgestatteten Räumlichkeiten arbeitet.

**(3.3) Verschlüsselung:**

Daten (etwa in E-Mails oder Datenbanken) werden so codiert, dass Unbefugte sie nicht lesen können. Prozesse zur Verschlüsselung von Datentransfer und -speicherung, einschließlich der Sicherheit der Systeme und des entsprechenden Krypto-Konzeptes.

**(4) Fazit:**

Vertraulichkeit ist der Eckpfeiler des modernen Datenschutzes und der Datensicherheit. Ohne wirksame Barrieren gegen unbefugte Zugriffe verliert jedes System seine Integrität und das Vertrauen der Nutzer. Nur wer weiß, dass seine sensiblen Daten geschützt sind, nutzt digitale Dienste angstfrei. Dabei gilt, der Aufwand muss in einem gesunden Verhältnis zum Umfang der Verarbeitung stehen ([Art.32 DS-GVO](#)).

In einer zunehmend vernetzten Welt mit Cloud-Diensten und künstlicher Intelligenz reicht es nicht mehr aus, Daten nur oberflächlich zu schützen. Vertraulichkeit muss bereits beim Design von Systemen integriert sein (Privacy by Design), um den wachsenden Cyber-Bedrohungen dauerhaft standzuhalten.

**g) 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 von den Verantwortlichen und den Auftragsverarbeitern geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten mit der Fähigkeit, die Verfügbarkeit der personenbe-

zogenen 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-Kreditanspruchs oder Online-Einstellungsverfahrens 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 von und durch die Verantwortlichen zu melden. Nur wenn kein 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. Auskunft), oder der Einholung von Einwilligungen bei Zweckänderung der ursprünglich erhobenen Daten



### (4) 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.

## **h) Verfügbarkeit (Datenschutz mit Sicherheit)**

### **(1) Ziel:**

Mit dem Ziel der Verfügbarkeit im Datenschutz ist sicherzustellen, dass personenbezogene Daten und die zugehörigen IT-Systeme für befugte Personen jederzeit vorhanden, abrufbar und funktionsfähig sind. Dies bedeutet zu jeder Zeit den unverzüglichen Zugriff auf, die Auffindbarkeit der (personenbezogenen) Daten und der Verarbeitung im ordnungsgemäß vorgesehenen Prozess, einschließlich einer angemessenen, gut verständlichen Darstellung für die Person (Datenmanagement – Systeme, Datenbanken, Suchfunktionen). Dies bedeutet ein Schutz und zügiger Zugriff auch bei physischen oder technischen Zwischenfällen und bei hoher Systemlast. Bei der Ausnahme eines Störfalles sind und werden Maßnahmen zur Behebung getroffen.

### **(2) Rechtliche Anforderungen:**

#### **(2.1) Begrenzung**

Nach den Grundsätzen für die Verarbeitung personenbezogener Daten in [Art.5 Abs.1e\) DS-GVO](#) dürfen diese in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Bei entsprechenden Schutzmaßnahmen gelten Ausnahmen ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke ("Speicherbegrenzung").

#### **(2.2) Sicherheit**

Nach den Vorgaben zur Sicherheiten der Verarbeitung in [Art.32 Abs.1 in Verbindung mit 1b\)](#) sind 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 von den Verantwortlichen und den Auftragsverarbeitern geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen gegebenenfalls u. a. die Fähigkeiten der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen ein.

#### **(2.3) Information und Auskunft**

Nach den [Art. 13 und 14 DS-GVO](#) ist bei Erhebung von personenbezogenen Daten die Person - IMMER - zu informieren, unabhängig der direkten Erhebung bei den betroffenen oder über Dritte. Jeder Person steht nach [Art.15 DS-GVO](#) ein Auskunftsrecht über die erhobenen und gespeicherten Daten – jederzeit – zu. Sofort bei direkter Erhebung bei der betroffenen Person, innerhalb einer angemessenen Frist, maximal nach einem Monat bei Erhebung von Dritten, und die Auskunft ist unverzüglich spätestens nach einem Monat nach Anfrage zu erteilen. ([Fristen nach Art.12 Abs.3 DS-GVO](#))

#### **(2.4) Datenübertragung**

Die betroffene Person hat nach [Art.20 DS-GVO](#) das Recht, die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und diese Daten einem anderen Verantwortlichen ohne Behinderung übermitteln zu können.

### **(3) Praktische Anforderungen:**

(3.1) Routine:

Wichtig ist eine Routine (auch Prozess genannt) zu entwickeln für:

- ✓ Die Erhebung, spätere Löschung und den jederzeitigen Abruf von Daten zu einer Anfrage der Betroffenen.
- ✓ Die Erstellung regelmäßiger Backups, am besten über mehrere Zeitpunkte, falls sich mal ein Virus zwischendurch eingeschlichen haben sollte. Zur Sicherheit sollten diese Backups außerhalb der laufenden Systeme, also extern oder in einer Cloud aufbewahrt werden. Im Ernstfall sollen diese ja der Wiederherstellung dienen.
- ✓ Die regelmäßige Wartung und Prüfung wie Installation von Updates zur Erhaltung fehlerfreier Systeme und Software,

(3.2) Kernkompetenzen:

- ▶ **Prävention:** Redundante Systeme (RAID, Cluster) und unterbrechungsfreie Stromversorgungen (USV) minimieren das Risiko von Ausfällen.
- ▶ **Detektion:** Kontinuierliches Monitoring erkennt Engpässe und Angriffe, bevor sie zu kompletten Stillständen bei Systemausfällen führen.
- ▶ **Reaktion:** Ein erprobtes Backup-Konzept (z. B. nach der 3-2-1-Regel) und klare Notfallpläne (Disaster Recovery) garantieren eine schnelle Wiederherstellung.

(4) Fazit:

Die Verfügbarkeit von Daten hat sich von einer rein technischen IT-Anforderung zu einer rechtlichen und existenziellen Notwendigkeit entwickelt. Während der Datenschutz klassischerweise oft mit dem Schutz vor unbefugtem Einblick (Vertraulichkeit) gleichgesetzt wird, zeigt die Praxis, dass der Verlust oder die Blockade von Daten – etwa durch Ransomware - Angriffe, Hardwareausfälle oder Naturkatastrophen – oft die schwerwiegenden wirtschaftlichen und gesellschaftlichen Folgen hat. Ein moderner Datenschutz ist nur dann wirksam, wenn er die Handlungsfähigkeit von Organisationen sichert und gleichzeitig die Rechte der Betroffenen wahrt, jederzeit auf ihre Daten zugreifen zu können.

Verfügbarkeit im Datenschutz bedeutet digitale Resilienz. Nur wer seine Daten nicht nur schützt, sondern sie auch im Krisenfall verlässlich bereitstellen kann, erfüllt die gesetzlichen Anforderungen der DS-GVO und sichert langfristig das Vertrauen von Kunden, Mitarbeitern und Partnern.

i) Wer verantwortet den Datenschutz?

|                                                              |                                                                  |
|--------------------------------------------------------------|------------------------------------------------------------------|
| <input type="checkbox"/> Der Konzern / das Mutterunternehmen | <input type="checkbox"/> Die Geschäftsführung                    |
| <input type="checkbox"/> Das Unternehmen / die Organisation  | <input type="checkbox"/> Die Datenschutzbeauftragten             |
| <input type="checkbox"/> Die Webmaster                       | <input type="checkbox"/> Die Informationssicherheitsbeauftragten |

\*)Versuchen Sie es, die Antworten stehen weiter unten

(1) Ziel:

Mit der gesetzlichen Regelung zum Verantwortlichen verfolgt der Datenschutz im Wesentlichen das Ziel der Sicherstellung einer klaren Haftungsstruktur, um betroffenen Personen die Möglichkeit zu geben, ihre Rechte effektiv durchsetzen zu können. Mit:

- ✓ der eindeutigen Zuordnung von Pflichten,
- ✓ der Schaffung eines zentralen Ansprechpartners für Betroffene und
- ✓ einem Adressat für alle Angelegenheit der Aufsichtsbehörden.

(2) Rechtsgrundlage:

Nach Art.4 Abs.1 Nr.7 DS-GVO ist:

"Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die

allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

und ein Vertreter der/des Verantwortlichen nach [Art.4 Abs.1 Nr. 17 DS-GVO](#) ist:

*"Vertreter" eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß [Artikel 27 DS-GVO](#) bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern ([Art.27 Abs.1 DS-GVO](#)), Abs.2 nennt wenige Ausnahmen)*

- ✓ Der Vertreter muss in einem EU-Land niedergelassen sein, das im Zusammenhang mit den angebotenen Waren und Dienstleistungen steht (Art.27 Abs.3)

*Die Benennung erfolgt unbeschadet etwaiger rechtlicher Schritte gegen den Verantwortlichen oder den Auftragsverarbeiter selbst (Art.27 Abs.4)*

- ✓ Die Vertretungsregelung gilt nur für Vertreter von nicht in der EU niedergelassenen Verantwortlichen oder Auftragsverarbeitern

### (3) **Praktisch:**

#### (3.1) Verantwortlich ist:

Das Unternehmen, die Organisation, die Juristische Personen (wie eine GmbH oder AG) oder natürliche Personen (bei Einzelunternehmen) die über die Zwecke und Mittel der Datenverarbeitung entscheiden und für die Einhaltung<sup>6</sup> haften.

Der Vorstand oder Geschäftsführer muss die Einhaltung des Datenschutzes sicherstellen und die Aufsicht darüber führen, auch durch Schaffung einer geeigneten Organisation und Maßnahmen. Diese Pflicht ist nicht delegierbar<sup>7</sup> und kann auch nicht von einer Obergesellschaft übernommen werden.

#### (3.2) Nicht verantwortlich sind:

- ✗ die Informationssicherheitsberater, da verantwortlich für die IT-Sicherheit
- ✗ die Webmaster, da verantwortlich für Betrieb, Wartung und Sicherheit der Website
- ✗ die Datenschutzbeauftragten, da keine Entscheider, sondern Berater im Datenschutz.

### (4) **Mitverantwortliche im Datenschutz?**

#### (4.1) Auftragsverarbeiter:

##### (4.1.1) Definition:

Auftragsverarbeiter sind natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die personenbezogene Daten nur im Auftrag der Verantwortlichen verarbeiten, ohne Verbindung zu Betroffenen und damit nur für diese Verarbeitung der Verantwortliche

##### (4.1.2) Rechtsgrundlage:

Nach [Art.4 Abs.1 Nr.8 DS-GVO](#) ist:

der "Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

[Art.28 DS-GVO](#) ergänzt die Pflichten des Auftragsverarbeiters gegenüber den Verantwortlichen. In Bezug auf die beauftragte Datenverarbeitung gilt die Einhaltung der gesetzlichen und ggf. vertraglichen Regelungen, der Unterstützung des Verantwortlichen gegenüber den Betroffenen und den Aufsichtsbehörden, Offenlegung und Kontrollmöglichkeiten der Art der Verarbeitung und Sicherheit.

##### (4.1.3) Praktisch:

Auftragsverarbeiter ist, wer im Auftrag und nach Weisung Daten verarbeitet, die dem Daten-

<sup>6</sup> Quelle: SITTIG LAW Kanzlei Blog [„Wer ist für die Einhaltung des Datenschutzes im Unternehmen verantwortlich?“](#)

<sup>7</sup> Quelle: activeMind.AG [„Verantwortung, Haftung und Delegierbarkeit des Datenschutzes im Unternehmen“](#)

schutz unterliegen. Kernpunkte sind:

- ▶ Strikte Weisungsgebundenheit: Daten dürfen ausschließlich auf dokumentierte Weisung des Verantwortlichen verarbeitet werden<sup>8</sup>.
- ▶ Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu bieten.
- ▶ Unterstützung der Verantwortlichen in Bezug auf Betroffenenrechte, Meldung von Datenpannen und geeignete Information für die Erstellung einer Datenschutz-Folgenabschätzung bereitstellen.
- ▶ Führung eines Verzeichnisses von Verarbeitungstätigkeiten einschließlich Subunternehmen
- ▶ Rückgabe und Löschung von Daten gemäß Auftrag.

#### (4.2) Gemeinsam Verantwortliche?

##### (4.2.1) *Definition:*

Eine gemeinsame Verantwortlichkeit (auch mehrere Parteien) liegt vor, wenn die beteiligten Stellen zusammen bestimmen, warum (Zweck) und wie (Mittel) personenbezogene Daten verarbeitet werden. Im Gegensatz zur Auftragsverarbeitung entscheidet der Partner hier nicht nur weisungsgebunden, sondern bestimmt aktiv mit (eben gemeinsam)<sup>9</sup>.

##### (4.2.2) *Rechtsgrundlage:*

Nach [Art.26 DS-GVO](#) „Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt“ (Abs.1) „Ungeachtet der Einzelheiten der Vereinbarung gemäß Absatz 1 kann die betroffene Person ihre Rechte im Rahmen dieser Verordnung bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen.“ (Abs.3) Es gibt keine Privilegierung gegenüber allen Verantwortlichen!!!

##### (4.2.3) *Praktisch:*

Klassische Beispiele sind Social-Media Unternehmensseiten, bekannt aus der EuGH Rechtsprechung zur Facebookseite<sup>10</sup>. Betreiber einer Facebook- oder Instagram - Seite und der Plattformbetreiber bestimmen gemeinsam, wie die Daten der Seitenbesucher verarbeitet und für Statistiken genutzt werden. Auch für gemeinsame Marketingkampagnen oder Veranstaltungen zählen dazu. Weiterführende Information bietet die Datenschutzkonferenz der Aufsichtsbehörden der Bundesländer im [Kurzpapier Nr. 16](#) oder die [Orientierungshilfe zur gemeinsamen Verantwortlichkeit](#) des bayerischen Landesbeauftragten für den Datenschutz.

### 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“<sup>11</sup> 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<sup>12</sup>

Cyberangriffe wirken oft wie „Magie“, viele Unternehmen scheitern aber an den Grundlagen, öffentlich erreichbare Administrator Ports, schwache Passwörter, keine Multi Faktor

<sup>8</sup> Quelle: Mittelstand Digitalzentrum Chemnitz „[Auftragsverarbeiter nach DS-GVO](#)“

<sup>9</sup> Quelle: Sächsische Datenschutz- und Transparenzbeauftragte: „[Gemeinsame Verantwortlichkeit](#)“

<sup>10</sup> Quelle: Dr. Datenschutz: „[Die gemeinsame Verantwortlichkeit im Sinn der DS-GVO](#)“

<sup>11</sup> Quelle: BSI „[Wegweiser im digitalen Alltag](#)“

<sup>12</sup> Quelle: Netzwelt.de: „[Hackerangriff auf Amazon: Sind eure Kundendaten jetzt in Gefahr?](#)“

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<sup>13</sup>**, 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<sup>14</sup>. Auszug aus dem Artikel:

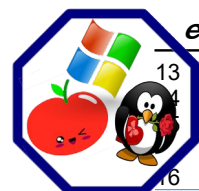
*Dortmund – Das slowakische IT-Sicherheitsunternehmen ESET hat eine neue Malware entdeckt. Die Schadsoftware trägt den Namen „PromptSpy“ und tarnt sich als Banking-App namens „MorganArg“ – eine Fälschung der offiziellen Chase/JPMorgan-Banking-App. Kriminelle verbreiten sie über gefälschte Webseiten.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



#### d) Meta – Instagram beendet verschlüsselte Direktnachrichten<sup>15</sup>

Meta schafft bei seinem Fotodienst Instagram die verschlüsselten Direktnachrichten ab. Die Begründung sei ein geringes Interesse der Nutzer. Eigentlich wollte Meta den Schutz privater Kommunikation nach Facebook und WhatsApp weiter ausbauen. Die bei Instagram erst vor wenigen Jahren eingeführte Funktion wird jetzt wieder abgeschafft. Laut Meta haben nur "sehr wenige" Menschen die verschlüsselten Chats genutzt, heißt es. Bevor die Funktion entfernt werde, sollten Anwender ihre bisherigen Chats und in Nachrichten geteilte Bilder sichern. Wer weiterhin verschlüsselt kommunizieren wolle, solle auf WhatsApp (Anm.: „Super Tipp 😬“) ausweichen, heißt es. Laut "The Verge" fordern Behörden weltweit strengere Regeln für Online-Plattformen. Kritiker argumentierten, dass verschlüsselte Nachrichten es erschwerten, strafrechtliche Inhalte zu erkennen und zu melden. Ein Generalstaatsanwalt in den USA habe einen Antrag eingereicht, Meta zu verbieten, verschlüsselte Chats für Minderjährige anzubieten. Auch in Großbritannien gebe es Diskussionen über mögliche Zugriffe auf verschlüsselte Daten, heißt es.



#### e) Trackt Microsoft illegal Minderjährige?<sup>16</sup>

- 13 Quelle: BSI *IT-Grundschutzkompendium NET.3.2. Firewall*  
 14 Quelle: Ruhr24.de: „*Experten warnen vor fremdgesteuerten Handys: „Banking-App“ bloß nicht runter laden*“  
 15 Quelle: techzeitgeist.de: „*Instagram beendet verschlüsselte DMs ab 8. Mai*“  
 16 Quelle: theverge.com: „*Instagram is getting rid of end-to-end encrypted DMs that 'very few' people used*“  
 16 Quelle: Netzpolitik.org: „*Österreichische Datenschutzbehörde: Microsoft hat illegal Minderjährige getrackt*“

Die österreichische Datenschutzaufsicht hat scheinbar auf einem Schülerrechner mit Microsoft 365 Education rechtswidrige Tracking-Cookies ausgemacht. Diese sollen rechtswidrig installiert und persönliche Daten abgegriffen haben, obwohl zuvor in den Datenschutzeinstellungen wo immer möglich die Datenübermittlung abgelehnt wurde. Das könnte auch für alle anderen „365er“ kritisch werden. Der Bekannte „Schrems“ mit seiner Organisation noyb ist bereits mit Beschwerden bei der Schule, Schulbehörde und Datenschutzaufsicht involviert. Wir werden davon noch lesen und hören, bestimmt!

#### f) Microsoft Word fliegt raus!<sup>17</sup>

Deutschland macht das OpenDocument Format (ODF) zur Pflicht für die öffentliche Verwaltung im Rahmen des „Deutschland-Stacks“, um die digitale Souveränität zu stärken und die Abhängigkeit von proprietären Formaten (wie .docx) zu beenden. Bis 2028 müssen Dokumente im Austausch in ODF oder barrierefreien PDF/UA-Formaten erfolgen (IT-Planungsrat im Standard Rahmenwerk „Deutschland-Stack“). Bis 2028 ist die gesamte öffentliche Verwaltung (Bund, Länder, Kommunen) umzustellen bzw. haben Dokumente in das ODF Format zu tauschen.

#### g) iPhone Update, jetzt aber!<sup>18</sup>



Der Spiegel berichtet über eine neue Angriffsmethode betreffend iPhones. Eine Schatten-Attacke raubt das ganze Handy aus. Der iPhone-Angriff sorgt für Aufsehen. Die Sicherheitsfirma Lookout hat mit DarkSword eine hochentwickelte Exploit-Kette entdeckt, die iPhones gezielt kompromittiert und dabei in Minuten nahezu sämtliche Daten ausliest, von Passwörtern über Chats und gespeicherte Telefonnummern bis hin zu Krypto-Wallets und WLAN-Passwörtern. Angriffe konnten bis November 2025 zurückverfolgt werden. Der Exploit nutzt die Sicherheitslücken sofort aus, sobald das Gerät die präparierte Webseite oder den Schadcode lädt und extrahiert Daten in wenigen Minuten. Danach wird der Exploit nicht dauerhaft auf dem Gerät sichtbar, sodass eine Infektion schwer zu erkennen ist. Betroffen sind laut den Experten in diesem Fall nur iPhones mit den iOS-Versionen 18.4 bis 18.7, also ältere Varianten. Deshalb:

- ✓ iOS regelmäßig aktualisieren
- ✓ Vorsicht bei unbekannten Webseiten
- ✓ Sicherheitsfunktion (z. B. den Blockierungsmodus) aktivieren

#### h) Neue Kreditfalle<sup>19</sup>



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 Banken 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.

#### i) Die gefährlichen Altgeräte<sup>20</sup>

Neues Smartphone, Tablett, Notebook oder PC? Alle Daten auf dem Altgerät, löschen,

Quelle: IT-Administrator: „[Öffentliche Verwaltung steigt auf ODF um](#)“

18 Quelle: SPIEGEL Netzwelt: „[Warum iPhone-Nutzer jetzt Updates einspielen sollten](#)“

19 Quelle: t3n: „[Neue Kreditfalle: So missbrauchen Betrüger das Postident-Verfahren](#)“

20 Quelle: PC-WELT: „[So gefährlich sind alte Geräte – entfernen Sie diese unbedingt aus Ihren Konten](#)“

Dokument von <https://volkerschroer.de>

überschreiben und auf Werkseinstellungen zurücksetzen! 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.

#### j) „Warum betrifft Cybersicherheit uns alle?“<sup>21</sup>

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.*

#### k) Microsoft, das nächste Support-Ende<sup>22</sup>

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! 😊

#### l) „Wenn der Datenschützer (ich) sauer wird!“

##### (1.1) Umstand:

Als Besitzer einer Minidrohone habe ich, auch wenn nicht erforderlich, bei „sicher.de“ (Name(n) geändert) eine Versicherung für die Drohnen-Nutzung abgeschlossen. Jetzt wollte ich mir die Vertragsdokumente auf der Internetseite anschauen ... WEG! 😞 ... Stattdessen werde ich aufgefordert, eine App aus dem Store herunterzuladen, um an die Dokumentation und alle weiteren Angaben zu kommen. 🗨️ Hinweis war, die „sicher.de“ ist jetzt zur „ganzsicher.de“ umgezogen. Gut (oder auch nicht), habe ich mir die App der „ganzsicher.de“ dann heruntergeladen. Neben umfangreichen Fragen zum Abschluss meines Profils in der App (die ich übersprungen habe), gab es keine Möglichkeit der Kündigung. Zum Stichwort „Kündigung“ hat der Chatbot auf die Produktseite verwiesen. Anrufen war nicht möglich, aber man konnte einen Telefontermin (pures Verkaufsmarketing, nehme ich an) für Vormittag oder Nachmittag vereinbaren. Sollte ich da etwa die ganze Zeit warten? Also war ich mal richtig „angefressen“ (= sauer 🤬).

##### (1.2) Fragen an die Datenschutzbeauftragten:

- ➡ Wann bitte habe ich meine Einwilligung zur Weitergabe der Daten gegeben?
- ➡ Wo bitte habe ich der Verlagerung des Zugriffs von der Website auf eine App zugestimmt?
- ➡ Wo bitte war die Kündigungsmöglichkeit bei Verweigerung der Zustimmung zu beidem?

<sup>21</sup> Quelle tagesschau.de „Cyberkriminalität“

<sup>22</sup> Quelle Microsoft: „End of support for Office 2021 → By or Try Microsoft 365“

(1.3) Antworten

- ❗ „Sicher.de“ wurde von „Ganzsicher.de“ der Muttergesellschaft übernommen, aber der Vertragspartner wäre unverändert „Sicher.de“ (???) und die Schwestergesellschaft „Sicherdigital.de“ würde die notwendigen IT-Dienstleistungen erbringen. Die operative Betreuung mit Auskünften, Vertragsänderungen und damit verbundene Kommunikation einschließlich Marketing würde jetzt im Konzern durch die Muttergesellschaft „Ganzsicher.de“ wahrgenommen. Nachlesbar in der Datenschutzerklärung der „Sicher.de“.
- ❗ Keine Zustimmung erforderlich, da a.) Vertragserfüllung ([Art.6 Abs.1b DS-GVO](#)) und b.) „berechtigtes Interesse“ ([Art.6 Abs.1f DS-GVO](#)) bei Konzerngesellschaften.

(1.4) Was war falsch?

- ❌ Mal davon abgesehen, dass alleine ein Wechsel des Kommunikationsmediums (Website zu Smartphone-App) an sich schon jeden Verbraucherschützer auf die Palme bringt.
- ❌ Bei der Frage nach dem aktuellen Vertragspartner fehlt noch jede klare Aussage. Wenn es – wie behauptet – noch „Sicher.de“ ist, fehlt jeder Hinweis bzw. Zugriff.
- ❌ Die Muttergesellschaft als aktueller und einziger Kommunikationspartner „Ganzsicher.de“ ist nicht in der Datenschutzerklärung aufgeführt, nur die „Sicherdigital.de“

(1.5) Konzernprivileg DS-GVO ??

In der DS-GVO gibt es kein allgemeines Recht, personenbezogene Daten beliebig zwischen Muttergesellschaften, Tochtergesellschaften oder Schwestergesellschaften auszutauschen. Diese Datenverarbeitungen innerhalb eines Konzerns gelten nicht automatisch als „intern“. Vielmehr ist jedes Konzernunternehmen wie eine separate, „fremde“ Firma, also als ein Dritter zu behandeln und ist jeweils ein eigener „Verantwortlicher“ nach [Art. 4 Nr. 7 DS-GVO](#). In der Konsequenz müssen Datenverarbeitungen zwischen Konzerngesellschaften individuell auf eine gesonderte Rechtsgrundlage gestützt werden. Die einzelnen Unternehmen bleiben gleichwohl eigenständige Verantwortliche im Sinne der DS-GVO.

Die Rechtsgrundlage „**berechtigtes Interesse**“ erlaubt eine Datenübermittlung gemäß dem [Erwägungsgrund 48 zur DS-GVO](#) innerhalb des Konzerns nur zu internen Verwaltungszwecken („Kleines Konzernprivileg“). Es ist kein gesetzliches Sonderrecht, sondern beschreibt Erleichterungen für die Datenübermittlung innerhalb von Unternehmensgruppen nach der DS-GVO. Es erlaubt Konzerngesellschaften, personenbezogene Daten für rein interne Verwaltungszwecke (wie zentrale Personalverwaltung, Konzern-IT oder Controlling) auszutauschen. **Es ist kein Freifahrtsschein** und darf nicht für Werbezwecke oder abteilungsübergreifenden, kommerziellen Datenaustausch genutzt werden, dazu Bedarf es einer Einwilligung.

(1.6) Konsequenz:

Das ist ein praktisches Beispiel, wo sich der verärgerte Kunde, aber spätestens die Verbraucherzentrale an die Versicherungs- und Datenschutzaufsicht wendet. Es kann z. B. so kommen- 😊.

m) 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.<sup>23</sup>

(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

23 Quelle: heise.de: „[Anthropics neues KI-Modell Mythos: Zu gefährlich für die Öffentlichkeit](#)“  
Dokument von <https://volkerschroer.de>

Konsequenzen haben.<sup>24</sup> Trumps schärfste Waffe gegen uns ist ein Exportstopp.<sup>25</sup>

(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.<sup>26</sup>

n) 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.<sup>27</sup>

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 generierter Inhalte.

o) Personalausweis: Kein Pfand und Kopiereinschränkungen

Neben der DS-GVO gibt es auch ein Personalausweisgesetz, das mit Hinweisen auf der Webseite des Bundesministeriums des Inneren eingesehen werden kann<sup>28</sup>.

(1.1) Deutlicher Hinweis:

Der Umgang mit dem Personalausweis ist rechtlich deutlich enger begrenzt, als viele Organisationen in der Praxis annehmen. Die Leitlinien sind dabei klar: kein Kopieren ohne gesetzliche Grundlage, keine Archivierung von Kopien, kein Scannen und elektronisches Speichern, kein Einbehalten als Pfand, und in jedem Fall muss das Prinzip der Datenminimierung eingehalten werden.

(1.2) Warum:

Der Personalausweis enthält weit mehr Daten, als für die meisten Zwecke tatsächlich erforderlich sind. Neben Namen, Adresse und Geburtsdatum finden sich dort auch Lichtbild, Staatsangehörigkeit, Körpergröße, Augenfarbe, Zugangsnummer, Seriennummer und die maschinenlesbare Zone (MRZ). Also weit mehr als für den bestimmten Zweck notwendig ist, was gegen [Art.5 Abs.1c der DS-GVO](#) verstößt, da weder „angemessen“ noch „erheblich“.

(1.3) Dringende Empfehlung BMI:

**Schwärzen der Ausweiskopie:**  
Ausweisdaten, die nicht zur Identifizierung benötigt werden, können und sollen auf der Kopie vom Ausweisinhaber geschwärzt werden.



Bildquelle: Vorlagen beim Kraftfahrtbundesamt

Ausweisdaten, die nicht zur Identifizierung benötigt werden, können und sollen auf der Kopie von der Ausweisinhaberin oder von dem Ausweisinhaber geschwärzt werden. Das gilt insbesondere für die auf dem Ausweis aufgedruckte Zugangsnummer sowie für die Dokumentennummer, sofern nicht gesetzliche Regelungen diese Angaben erfordern, zum Beispiel das Geldwäschegesetz.

Ausweisinhaberrinnen und Ausweisinhaber sind auf die Möglichkeit und Notwendigkeit der Schwärzung hinzuweisen. Die geschwärzten Angaben sollten nicht mehr lesbar oder durch technische Verfahren wiederherstellbar sein. Nach Erfüllung des Verwendungszwecks sollte dafür Sorge getragen werden, dass die Ausweiskopie umgehend und datenschutzgerecht vernichtet wird, um eine missbräuchliche Verwendung zu verhindern

24 Quelle: tagesschau.de: „[Was die Sperre für die KI-Industrie bedeutet](#)“ und mehr

25 Quelle: focus.de: „[KI und andere Technologien: Trumps schärfste Waffe gegen uns ist ein Exportstopp](#)“

26 Quelle: Euronews.com: „[Nach OpenAI nun Anthropic: KI-Modelle griffen bei Tests auf externe Systeme zu](#)“

27 Quelle: digitalbusiness-magazin.de: „[Cyberangriff durch KI: Wie sich Unternehmen jetzt aufstellen müssen](#)“

28 Quelle: Bundesministerium des Inneren: „[Artikel Ausweiskopien](#)“

Sofern das Ausweisdokument im Original vorgelegt wird und die Identifizierung erfolgte, genügt in vielen Fällen die Anfertigung eines entsprechenden Vermerks. Eine zusätzliche Kopie des Ausweises ist in diesen Fällen nicht erforderlich.

 **p) Es liegt nicht am Datenschutz!**

Für alle Bereiche gilt: Unternehmen brauchen Rechtssicherheit, stabile wirtschaftspolitische Rahmenbedingungen und verlässliche Zukunftsperspektiven. Dass der Datenschutz eine Investitionsbremse sein soll, haben Forscher der Fraunhofer ISI eindeutig widerlegt<sup>29</sup>.

*„Weniger Datenschutz, mehr Innovation? Ein neues Policy Paper der vom Fraunhofer ISI koordinierten Plattform Privatheit zeigt, warum diese einfache Formel zu kurz greift. Die Autor:innen plädieren stattdessen für einen europäischen Weg, der Innovationsfähigkeit und Wettbewerbsstärke mit Datenschutz, Selbstbestimmung und digitaler Souveränität verbindet.“*

**Bei Bedarf, einfach mal sprechen!** 

<sup>29</sup> Quelle: [Fraunhofer-Institut für System- und Innovationsforschung ISI: „Innovation und Datenschutz“](https://volkerschroer.de)  
Dokument von <https://volkerschroer.de>